State of Michigan

CYBER DISRUPTION RESPONSE PLAN

October 2015

DTMB
Technology, Management & Budget

MICHIGAN STATE POLICE

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
MICHIGAN

State of Michigan
EXECUTIVE OFFICE
LANSING

RICK SNYDER
GOVERNOR

BRIAN CALLEY
LT.GOVERNOR

October 25, 2015

Dear Michigan Critical Infrastructure Partners:

Michigan government works diligently to block millions of unauthorized attempts to probe, scan, and access or disrupt its computer networks on a daily basis. These computer networks safeguard important information about Michigan's residents, control critical state agency operating systems, and provide customers with convenient access to state services. While the vast majority of these cyber anomalies are blocked by defensive systems, evolving threats represent a significant risk to the continuity of state government. Similar challenges are faced by Michigan's local government and private sector partners; organizations who also work diligently to safeguard their systems.

In 2011, Governor Rick Snyder introduced the Michigan Cyber Initiative to encourage a statewide effort among public and private partners to defend Michigan's critical networks. In support of this initiative, a team of state and local government representatives, alongside public safety and private sector critical infrastructure partners, developed the Michigan Cyber Disruption Response Strategy in 2013. To keep pace with the ever-evolving threats, we are proud to present the Michigan Cyber Disruption Response Plan.

The Plan provides guidelines to partner organizations to best protect Michigan's critical cyber infrastructure. The Plan includes strategies for information sharing, criminal investigation, cyber-attack response and recovery from a significant cyber-disruption to Michigan's critical infrastructure. Utilizing the Plan's strategies, participating organizations can collaborate in response to cyber threats as they are detected; often before the unthinkable happens.

It is our intent that by continuing to unify state government cyber security efforts, and working closely with our private sector and local government partners, we will continue Michigan's role as a national model of innovation, success and security.

Col. Kriste Etue

David Behen
DTMB Director and
State Chief Information Officer

Colonel Kriste Kibbey Etue
Director, Michigan State Police

Major General Gregory J. Vadnais
Adjutant General, Michigan National Guard

State of Michigan

CYBER DISRUPTION RESPONSE PLAN

Prepared by:
Department of Technology Management & Budget

10/25/2015

Table of Contents

This page intentionally left blank.

1.0 Executive Summary

The Michigan Cyber Disruption Response Plan (CDRP) was created to protect the health, safety, and economic interests of Michigan's residents and businesses by reducing the impacts of disruptive cyber related events through response and mitigation planning, awareness, and implementation. Cyber disruption events have the ability to severely impact the social, economic and physical welfare of state citizens and businesses through escalated or multiple simultaneously executed attacks on the state's most critical sectors. The plan provides a framework that enables state emergency management and information technology to work seamlessly with public and private partners to rapidly respond to and minimize the impact of cyber disruption events in Michigan.

This plan provides a common framework for identifying and responding to technological threats by defining five threat levels, that mirror the federal government model, with corresponding responses to address threats of increasing scope and severity. These cyber disruption threats range from minor malware incidents; through specific attacks on targeted state networks and services; to severe attacks capable of catastrophic impact to services and facilities of single or multiple sectors providing critical support to citizens government, public and private entities. The plan enables closely integrated planning by providing a standard incident response plan template for critical infrastructure entities and partnership use. It leverages technical training for core team members, well-planned and executed exercises, and risk based metrics to identify, implement and track continuous improvement initiatives.

2.0 Introduction

The Michigan Cyber Disruption Response Plan (CDRP) provides the primary emergency management (EM) and information technology (IT) agencies in Michigan with a broad framework to coordinate response and recovery operations in the event of disruption to state government critical cyber infrastructure. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, signed June 2013, identified 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste

- Transportation Systems
- Water and Waste Water Systems

3.0 Purpose

The CDRP provides EM, IT, and other potential stakeholders, within Michigan, a management framework to coordinate preparedness, response, and recovery activities related to a large-scale or long-duration cyber disruption. It incorporates IT personnel into the Michigan-wide Incident Command System (MI-ICS) structure.

4.0 Scope

The CDRP uses a framework to coordinate intra-Michigan cyber preparedness, response, and recovery activities. The CDRP coordinates closely with local security policies and procedures. It provides an expanded description of the plans and activities the Michigan Department of Technology, Management and Budget (DTMB), the Michigan National Guard (MING) and Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD), will implement to prepare for, respond to, and recover from large-scale cyber disruptions. The CDRP defines the Michigan Cyber Disruption Response Team (CDRT) as the active coordinating structure for cyber disruption incidents.

Cyber disruptions may be a single yet pertinent element of a larger incident that threatens lives, property, and continued operation of critical business functions. Activities conducted pursuant to this CDRP work within state and local planning and incident command structures, complement existing plans and procedures, and are compliant with the National Incident Management System (NIMS).

5.0 Cyber Disruption Response Plan Roles and Responsibilities

The State of Michigan government works with federal, state, and local agencies and organizations; education; and private industry to respond to, resolve, and address secondary effects of cybersecurity disruptions, manmade disaster or natural disasters. The state promotes collaboration between the respective cyber disruption response functions and emergency management functions of these various entities. Given the integration of information technology with virtually any other discipline or line of business, these two functions will have to be engaged in almost any type of disruption or emergency. Specific roles and responsibilities for each entity are defined in Annex E: CDRP Roles and Responsibilities.

6.0 Michigan Cyber Disruption Response Team (CDRT)

The CDRT is comprised of subject matter experts responsible for preparation, response to, and recovery from large-scale or long-duration cyber disruptions impacting Michigan’s critical infrastructure or other major assets. These disruptions could result from:

- Intentional threats (e.g., terrorism, internal or external)

- Accidental or unintended threats (e.g., disruption of power, shutdown of equipment, system patching without adequate testing)
- Process failures (e.g., institutionalized but untested processes)
- Natural phenomena (e.g., severe weather)

6.1 CDRT Membership and Organization

Department of Technology, Management and Budget (DTMB) and Michigan State Police (MSP) representatives will provide Cyber Disruption Response Team leadership. The Chief Security Officer (CSO) will be appointed Chairman and the Deputy State Director of Emergency Management and Homeland Security will serve as Vice Chairman. During State Emergency Operations Center (SEOC) activation, the Incident Commander directs CDRT operations.

6.1.1 CDRT Membership

The CDRT is composed of, at a minimum, representatives from the EM and IT communities from within Michigan. Other key federal, state, regional, local and private organizations, as necessary, may play a role in a Michigan's CDRT or may be enjoined as necessary (and to the extent possible) to assist in the operations of a CDRT.

The Michigan CDRT consists of two primary groups; a core entity and an extended group. The core entity provides the leadership, day-to-day operational management and emergency operations directions. This group is composed primarily of DTMB, MSP and MING leadership and staff. The extended group supports key planning, operational and technological expertise and support for their specific cyber systems, operations and facilities. The Michigan Cyber Civilian Corps (MiC3), consisting of volunteers from government, education and business sectors; provides a rapid response capability to Governor declared state of emergency cyber events. When activated, the MiC3 supports both the CDRT core and extended groups.

Michigan's CDRT members should meet the following requirements:

- CDRT core membership consists of key representatives from the EM, IT, and law enforcement communities.
- Member organizations will provide the appropriate level of decision-making authority to their assigned CDRT primary and alternate members.
- The CDRT chairperson determines the extent of team involvement based on incident scope and nature. Extended group representatives may only be included for incidents deemed to be within their area of expertise or business operations.
- The chairperson represents the CDRT in coordination with the Incident/Unified Commander and/or Operations or Planning sections during an incident response.

- The CDRT will appoint a chairperson and a vice-chair to oversee CDRT activities and communications.
- Additional local, state, and federal agencies, along with healthcare, education, and private sector partner organization members, with critical cyber infrastructure knowledge and expertise, may be requested to participate in applicable CDRT operations.

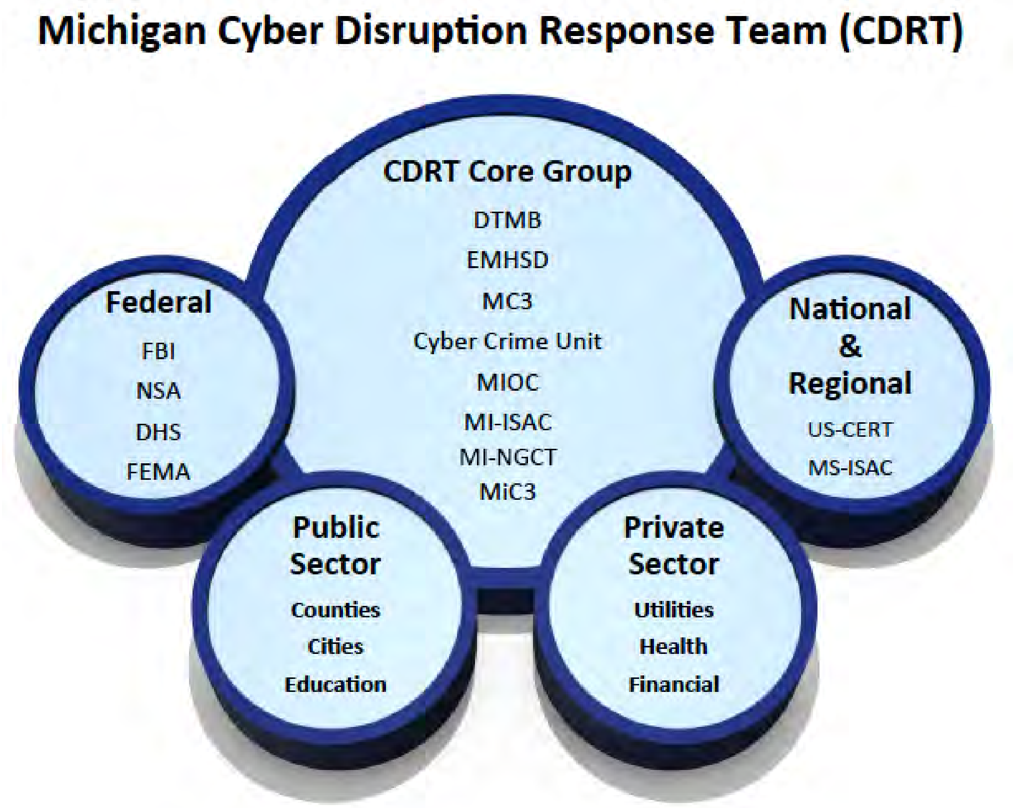
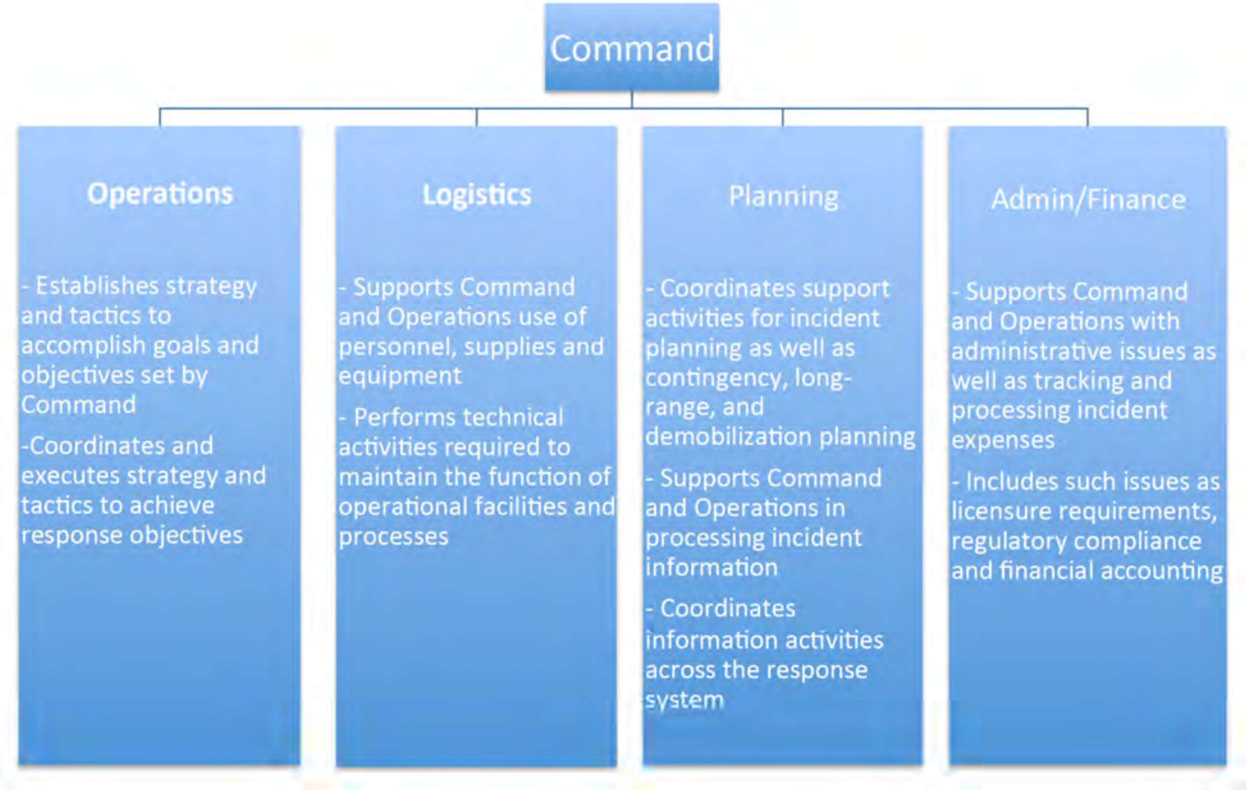


Figure 1: CDRT Membership

6.1.2 CDRT Organization

The CDRT internal structure follows Incident Command System (ICS) principles, with the Chair and Co-Chairs appointing a CDRT lead to act in the incident commander role. CDRT membership will fill Planning, Operations, Logistics, and Finance roles, as needed and as appointed by the CDRT lead.



Operations

- Establishes strategy and tactics to accomplish goals and objectives set by Command
- Coordinates and executes strategy and tactics to achieve response objectives

Logistics

- Supports Command and Operations use of personnel, supplies and equipment
- Performs technical activities required to maintain the function of operational facilities and processes

Planning

- Coordinates support activities for incident planning as well as contingency, long-range, and demobilization planning
- Supports Command and Operations in processing incident information
- Coordinates information activities across the response system

Admin/Finance

- Supports Command and Operations with administrative issues as well as tracking and processing incident expenses
- Includes such issues as licensure requirements, regulatory compliance and financial accounting

Image courtesy phe.gov

Figure 2: ICS Structure

As shown in Figure 3 on the following page, a CDRT may be established under the Planning or Operations Section. Under the Planning Section, it serves in a consultative role helping provide direction and expertise developing Incident Action Plan (IAP) objectives and related information. Under the Operations Section, the CDRT, or its members, may form a strike team or task force directing response/recovery actions or assisting in response/recovery actions in the field. The CDRT reports directly to the Incident/Unified Commander or other person responsible for directing response/recovery actions and providing specialized expertise to direct response efforts.

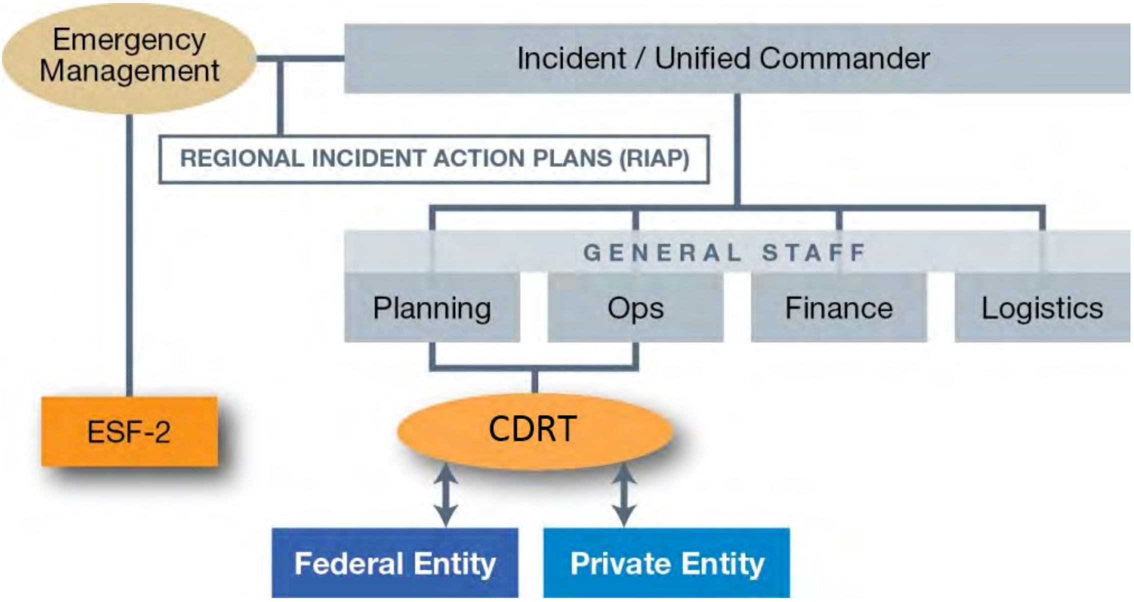


Figure 3: Organization Chart

6.2 Role of the CDRT

The CDRT is a specialized jurisdictional consultative group composed of representatives and subject matter experts from primarily the EM and IT domains. Representatives from other relevant domains are encouraged to participate. The CDRT serves the following roles in preparing for, responding to, and recovering from a cyber disruption:

- Helping executive management and Incident Command within the impacted systems and area understand the nature and potential duration of cyber disruptions.
- Helping EM staff determine the effects of cyber disruptions on critical life-safety systems, critical cyber assets, and other key response activities.
- Helping IT staff determine the potential resource needs of IT personnel and agencies to maintain, protect, and re-establish operations following a cyber disruption.

6.2.1 Preparation

The CDRT has a responsibility to be active in pre-event planning activities that increase the resilience of critical cyber assets across Michigan. The CDRT will:

- Identify threats and vulnerabilities to IT networks with respect to emergency management objectives and priorities.
- Identify mitigations (e.g., plans, procedures, hardening measures) for threats and vulnerabilities.
- Develop communications means and methodologies to enable intra- and extra-CDRT communication and transactions as prescribed in Annex A: Communication.

- Develop plans and procedures to address specific disruptions as described in Annex B: Response Plans.
- Train and exercise this CDRP, as well as other business continuity, continuity of operations, and continuity of government plans. Details on training and exercise program development and implementation are provided in Annex C: Training and Exercises.
- When necessary and possible, communicate with other CDRT representatives in the region to exchange best practices and information pertinent to preparing for cyber-related incidents.

6.2.2 Response

The core Cyber Disruption Response leadership team activates a virtual team of CDRTs as needed to support response activities. The CDRT incident response triage process seamlessly activates the SEOC during Severe and High Level incidents. The CDRT triage process is responsible for and manages the following activities:

- Monitor disruption events to determine scale and scope, and to determine if the event is stable, improving, or expanding.
- Share information within or between CDRTs that may indicate the development of a larger or more regional-level disruption event.
- Provide other CDRT representatives in the region with situational awareness and assistance during a catastrophic incident as necessary and possible.
- Help coordinate IT-related response activities pursuant to an Incident Action Plan (IAP) (Annex A, Figure A-2).
- Coordinate with EM support staff to procure critical cyber-related resources.
- Provide situational awareness and subject matter expertise and solutions for an Incident/Unified Commander and his/her General Staff during a response, including:
    - Assisting Incident/Unified Commander’s Operations Staff to understand technical and operational issues regarding cyber-related resources and networks.
    - Assisting Incident/Unified Commander’s Planning Staff in the development of priorities and objectives of a long-term response to a large-scale cyber disruption incident. Developing objectives and activities become the key elements of an action plan for a determined operational period, set out by the Planning Chief and staff for the Incident/Unified Commander and contained in an IAP.

6.2.3 Recovery

CDRTs have a responsibility to be active throughout the recovery phase of an event, under the direction of the Deputy State Director of Emergency Management and

Homeland Security. It is possible that the recovery effort could exist over an extended period of time. CDRT responsibilities include:

- Working with affected system owners to determine resources needed to restore operations to a normal state.
- Tracking restoration efforts and providing information to the Incident/Unified Commander's Operations Staff regarding estimated and actual time to full restoration.
- Working with emergency management recovery leads over the extended life of the recovery effort.
- Communicating with Michigan National Guard Joint Operations Center (MING JOC); providing situational awareness and determining if MING resources can be of assistance.
- Conducting internal and external CDRT after-action reviews to obtain lessons learned following an incident.

6.3 CDRT Operation

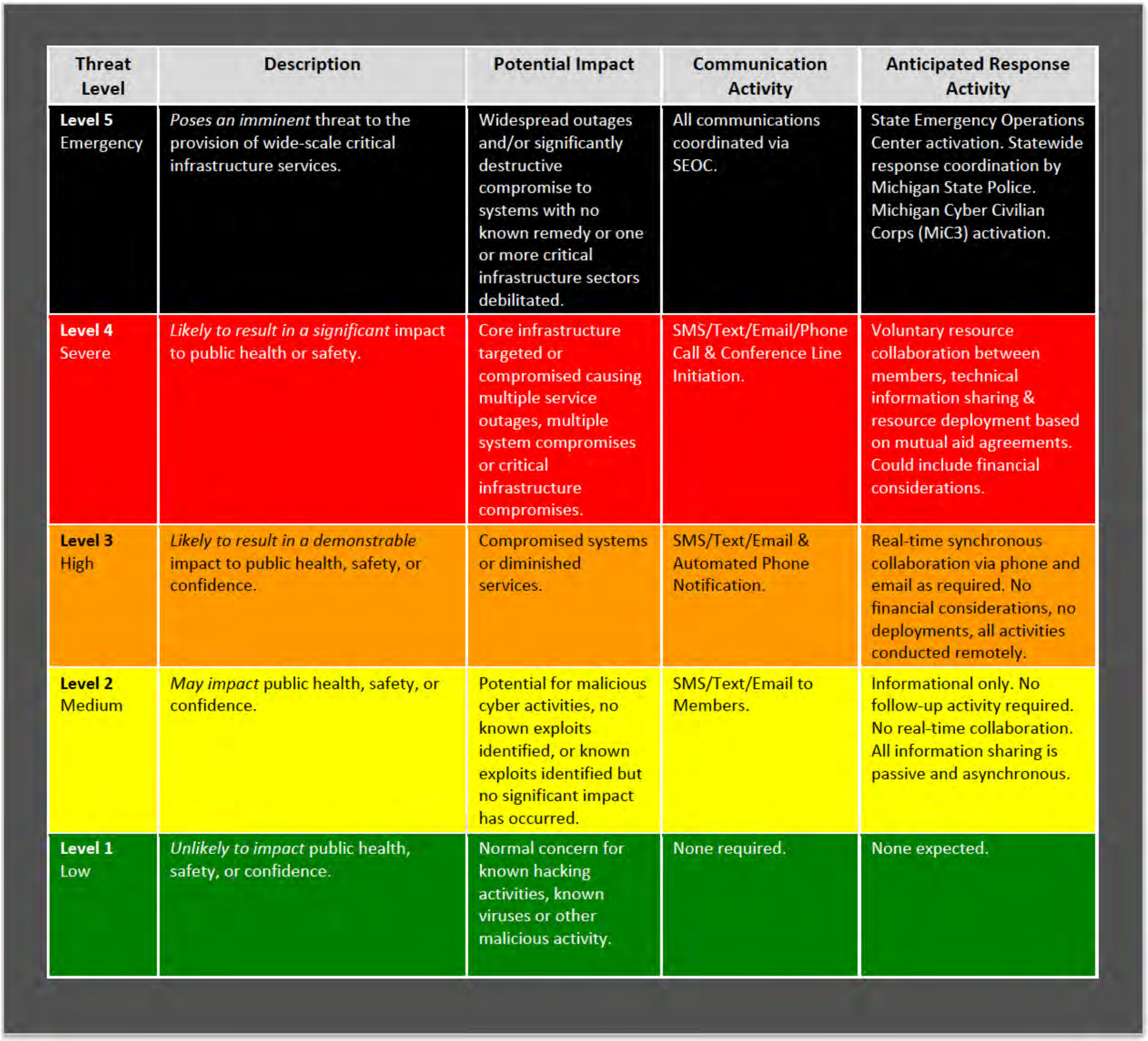
The CDRT chairperson will be the primary decision-maker on behalf of the CDRT. The chairperson has the ability to appoint staff to provide support to a cyber disruption response effort, including staff responsible for Operations, Planning, Logistics, and Finance, according to ICS principles.

The CDRT chairperson and staff, as appropriate, will direct CDRT efforts by:

- Identifying and communicating the role of the CDRT within the larger response effort.
- Understanding and documenting the situation.
- Developing objectives, goals and mitigation strategies.
- Setting operational periods (OPs) to organize resources and measure effectiveness.
- Assigning staff to consultative, mitigation, or corrective response and recovery roles.
- Identifying and communicating potential health and safety hazards.
- Conducting other duties required to complete the response and recovery effort.

7.0 Cybersecurity Alert Escalation/De-escalation Procedures

The Michigan Cybersecurity Threat Matrix consists of five distinct threat levels, as illustrated in Figure 4, which are impacted by internal and external cybersecurity events. The matrix provides a high-level snapshot of the communication and anticipated response activities for each threat level.



Threat Level	Description	Potential Impact	Communication Activity	Anticipated Response Activity
Level 5 Emergency	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services.	Widespread outages and/or significantly destructive compromise to systems with no known remedy or one or more critical infrastructure sectors debilitated.	All communications coordinated via SEOC.	State Emergency Operations Center activation. Statewide response coordination by Michigan State Police. Michigan Cyber Civilian Corps (MiC3) activation.
Level 4 Severe	*Likely to result in a significant* impact to public health or safety.	Core infrastructure targeted or compromised causing multiple service outages, multiple system compromises or critical infrastructure compromises.	SMS/Text/Email/Phone Call & Conference Line Initiation.	Voluntary resource collaboration between members, technical information sharing & resource deployment based on mutual aid agreements. Could include financial considerations.
Level 3 High	*Likely to result in a demonstrable* impact to public health, safety, or confidence.	Compromised systems or diminished services.	SMS/Text/Email & Automated Phone Notification.	Real-time synchronous collaboration via phone and email as required. No financial considerations, no deployments, all activities conducted remotely.
Level 2 Medium	*May impact* public health, safety, or confidence.	Potential for malicious cyber activities, no known exploits identified, or known exploits identified but no significant impact has occurred.	SMS/Text/Email to Members.	Informational only. No follow-up activity required. No real-time collaboration. All information sharing is passive and asynchronous.
Level 1 Low	*Unlikely to impact* public health, safety, or confidence.	Normal concern for known hacking activities, known viruses or other malicious activity.	None required.	None expected.

Figure 4: Michigan Cybersecurity Threat Matrix

The Cyber Disruption Response Escalation Path (Figure 5, below) depicts the state of Michigan decision-making process designed to drive rapid and effective responses to potential cyber disruption scenarios. The following sections define the escalation and de-escalation process for each cybersecurity threat level.

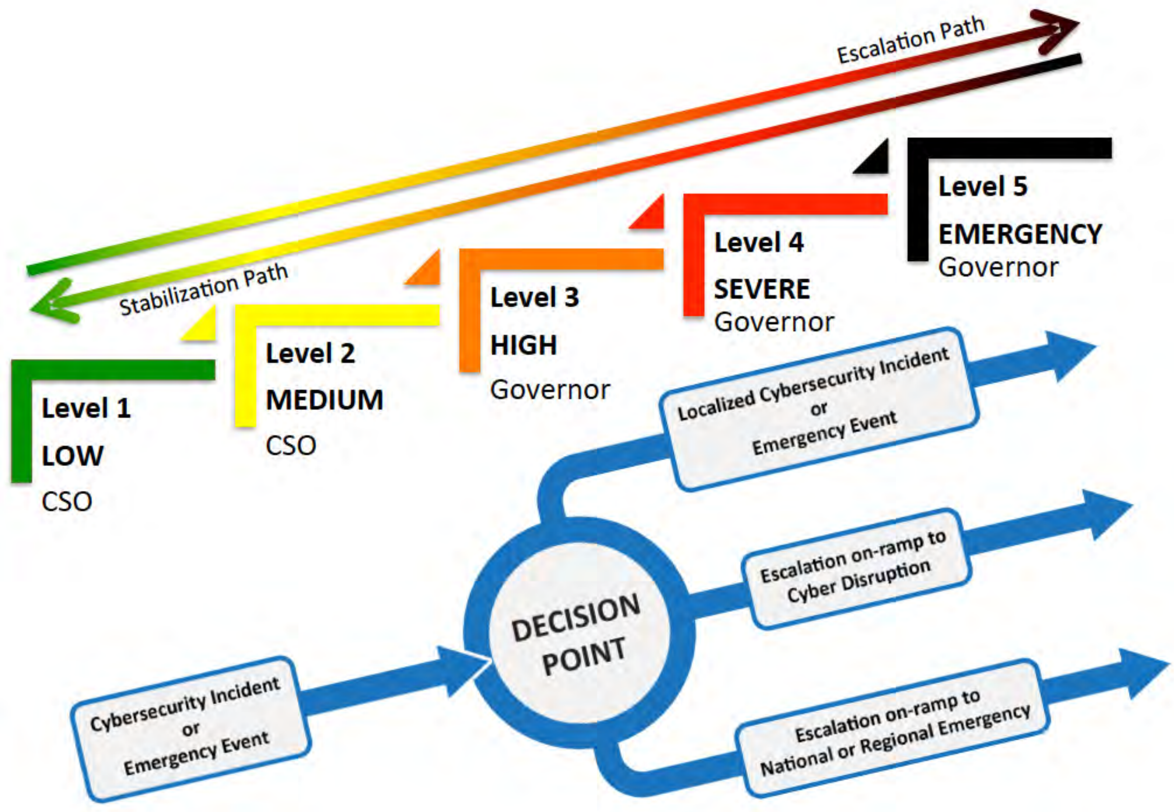

Escalation Path
Stabilization Path
Level 1
LOW
CSO
Level 2
MEDIUM
CSO
Level 3
HIGH
Governor
Level 4
SEVERE
Governor
Level 5
EMERGENCY
Governor
Localized Cybersecurity Incident or Emergency Event
Escalation on-ramp to Cyber Disruption
Escalation on-ramp to National or Regional Emergency
DECISION POINT
Cybersecurity Incident or Emergency Event

Figure 5: Cyber Disruption Response Escalation Path

This section provides the following information for each threat level:

- Level Definition – A brief description of what each security level means.
- Escalation/De-escalation Criterion – Descriptions of variables required to be in place for the alert level changes.
- Potential Impact – How the level impacts the state's agencies, business partners, local governments, and citizens.
- Communication Procedures – How the CSO communicates to individuals and organizations impacted by cybersecurity events.
- Responsibilities – This section describes what each group within the state needs to do to ensure that governmental IT operations are functioning during each level.

  Note: Threat levels in this document are based on the risk an event poses and the impact it has on the state government enterprise. Incidents may require the CSO to skip levels, to address a different threat, and return to the originating level after that threat has been mitigated.

7.1 Cybersecurity Threat Level 1 - Low (Green)

Level 1 – Low (Green) is the lowest operational level in the cybersecurity threat matrix. The following explains what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

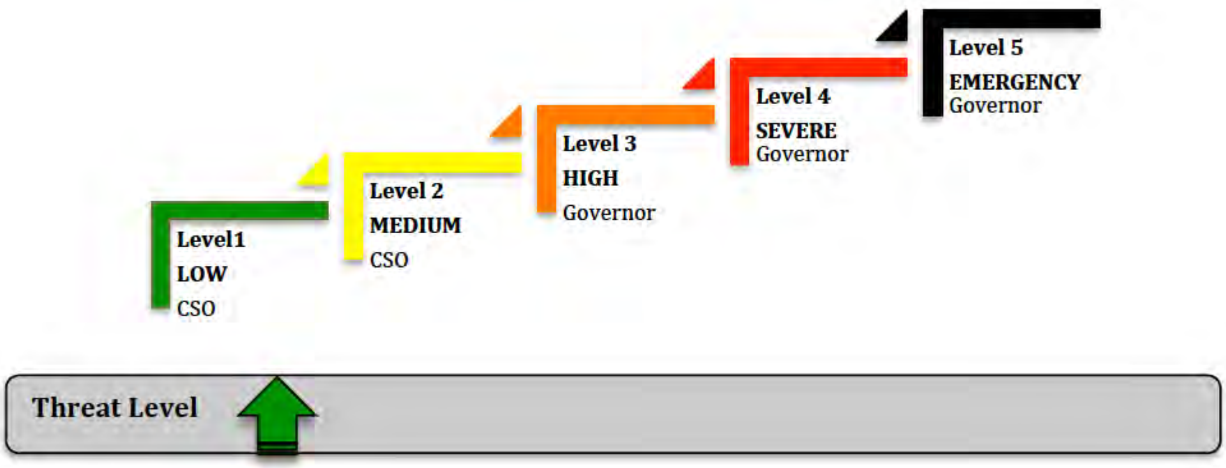


Figure 6: Level 1 – Low (Green)

7.1.1 Level Definition

Insignificant or no malicious activity has been identified. Examples include but not limited to:

- Credible warnings of increased probes or scans discovered in State of Michigan networks.
- Infected by known low risk malware.
- Other like incidents.
- Normal activity with low level of impact.

Actions:

- Continue routine preventative measures including application of vendor security patches and updates to anti-virus software signature files on a regular basis.
- Continue routine security monitoring.
- Determine baseline of activity for the state – it is important to know what "normal" looks like – and then continually be on alert for any changes to that baseline.
- Ensure all personnel receive proper training on cybersecurity policies and security best practices.

7.1.2 Escalation Criterion

Infrastructure is operating normally and there are no major known cyber threats on the horizon.

7.1.3 De-Escalation Criterion

In order to return to this level, the conditions that caused the change must be remediated.

7.1.4 Potential Impact

A Low threat level means no cyber related issues should be impacting state IT resources.

Note: Any type of IT disruption or anomalies noted on a State of Michigan network will be reported to the CSO so a determination can be made as to whether the disturbance is cybersecurity related or caused by planned IT related functions such as patch management or firewall reconfiguration.

7.1.5 Communication Procedures

Besides day-to-day operational communications, no special communication procedures are required while the state is at this level.

7.1.6 Responsibilities

When the state is at this level the following groups will be active and carry out their assigned duties:

- CSO – The CSO is responsible for the following functions:
    - Threat Monitoring – The CSO will monitor the national and international cybersecurity threat levels and cybersecurity informational resources to identify and report on potential threats that could impact the state.
    - Cybersecurity News and Information Sharing – The CSO will use the cybersecurity portal and the Michigan Information Sharing and Analysis Center (MI-ISAC) to post information on emerging cybersecurity threats and ways to combat them.
    - Email Notifications – The CSO will provide cybersecurity news and updates to members via email.
    - Log Validation – The CSO will review the security logs to determine if there are any suspicious network activities, such as bot, spyware, malware, or virus infections.
    - Validation Assessments – The CSO will use vulnerability and penetration tools to ensure that agencies have the most recent patches and antivirus agents, engines, and definitions.
    - White Hat Hacking – The CSO will proactively try to hack state IT resources to discover potential flaws that could lead to data breaches, hijacking, theft of services, and other exploits.
    - Anomaly Investigation – The CSO will investigate reports of network issues, such as slowdowns, disconnections, and disrupted services, to determine if the cause of the problem is due to technical issues or a cyber-attack.

    - MSP – The CSO will support MSP/EMHSD, Michigan Cyber Command Center (MC3) and Michigan Intelligence Operation Center (MIOC) with their cybersecurity missions.
    - MING – The CSO may coordinate with the National Guard to facilitate information sharing and resource preparedness.
    - State Government Service Providers Security Operations and Support (Provider SOS) – The CSO will work with work with the Provider SOS to identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies and users.
    - The CSO is responsible for installing and monitoring server-based security agents on servers located in the Enterprise Data Center (EDC). The CSO will also be responsible for:
        - 24/7 Hotline – Provider SOS will provide 24/7 security support for EDC and state agencies.
        - Managing Enterprise Firewalls – Provider SOS will monitor the enterprise firewall logs to ensure firewalls are in place and working properly and assist the CSO with firewall blocks against IPs that pose a threat to the network.
        - Reporting Incidents – Provider SOS will report all cybersecurity incidents to the CSO for investigation.
- The EDC is responsible for managing the enterprise servers in the server farm and the security agents that are installed on them. During Level 1 the EDC will be responsible for:
    - Patch Management – The EDC will ensure that all of the enterprise severs have the most current operating system patches installed on them and that the patch is installed correctly as defined by Security Benchmarks.
    - Antivirus Agents/Antivirus Signatures – The EDC will ensure that all of the enterprise severs have the most current antivirus security agents and that they are updated with the most current signatures. Any known discrepancies will be documented.
    - Internet Information Services (IIS) – The EDC ensures the IIS is in place, working properly and configured to Security Benchmarks. The Provider SOS also works with the EDC to monitor IIS logs for suspicious activity to report to the CSO for investigation.
    - Microsoft Operations Manager (MOM) – The EDC monitors MOM logs and alerts for server availability and out of the ordinary operating system level events to report to the CSO.
    - Firewall Management – The Provider SOS and the EDC monitor EDC firewall logs to ensure firewalls are in place and working properly. In

addition to this, the EDC will review and execute requested firewall changes.

- Information Security Officers (ISOs) – ISOs are responsible for working with the CSO to help identify and report on cybersecurity events that could impact their agencies' and the state's IT infrastructure. In addition to identifying potential cybersecurity events, the ISOs is responsible for:
    - Reporting Cybersecurity Incidents – ISOs are responsible for reporting agency specific cybersecurity incident(s) to the CSO using the Cyber Disruption Incident Report Form (Annex A, Figure A-3). Incidents can range from data breaches to unexplained network issues/traffic.
    - Agency Cybersecurity Alert Level – ISOs are responsible for monitoring their agencies' cybersecurity readiness and their internal threat level. This level should be increased when a confirmed cybersecurity incident occurs or during times the respective agency could be at greater risks of attack, such as tax season and elections.
- MSP (MC3, EMHSD) – MSP will continue to support the cyber mission by meeting with federal, state, and local government officials and state-based business owners to determine their cybersecurity readiness and communicating this information to the CSO and MIOC.
- MIOC – The MIOC works with the MC3, CSO, and Federal Bureau of Investigation (FBI) to identify potential threats that could impact the state and its business partners.

7.2 Cybersecurity Threat Level 2 - Medium (Yellow)

Level 2 – Medium (Yellow) is the first active threat level in cybersecurity threat matrix. The following explains what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

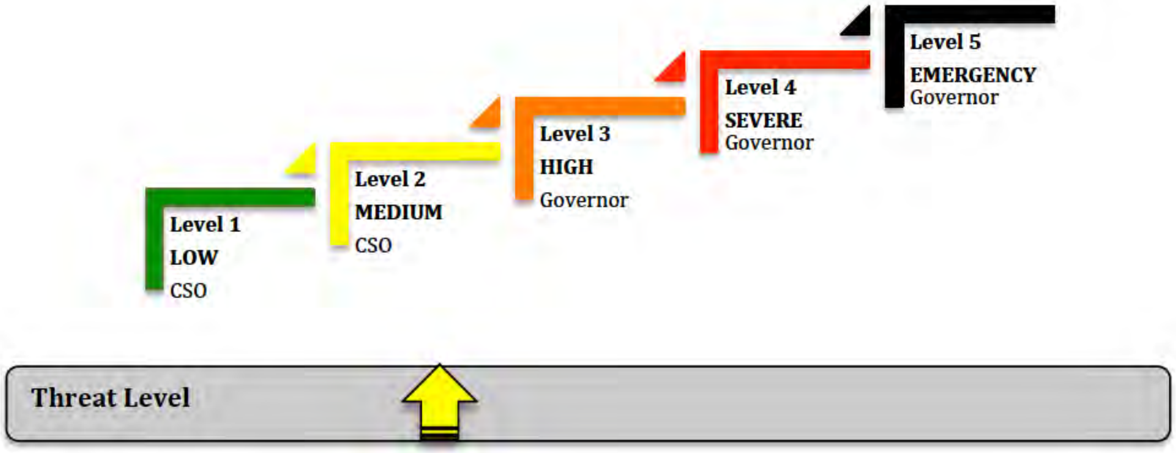


Figure 7: Level 2 – Medium (Yellow)

7.2.1 Level Definition

Malicious activity has been identified on State of Michigan networks with minor impact. Examples include but not limited to:

- Change in normal activity with minor impact to IT operations.
- A vulnerability is being exploited and there has been minor impact.
- Infected by malware with the potential to spread quickly.
- Compromise of non-critical system(s) that did not result in loss of sensitive data.
- A distributed denial of service attack with minor impact.

Actions:

- Continue recommended actions from previous level.
- Identify vulnerable systems and implement appropriate counter-measures.
- Identify malware on system and remediate accordingly.
- Document data exposure with minor impact.
- When available, test and implement patches, install anti-virus updates, and other security measures in next regular cycle.
- The Multi-State Information Sharing and Analysis Center (MS-ISAC) will be contacted for additional guidance.

7.2.2 Escalation

In order to raise the state or agency threat level to Level 2, the following conditions must be in place:

Risk Level – The threat is limited to one state agency, application, or website; and/or the risk of the threat is low and it can be easily remediated without having a long-term impact to state, business partners, local governments, and citizens.

7.2.3 Potential Impact

At Level 2, the following conditions are in place:

- Impact to IT Services
  - There is no threat to mission critical applications or resources; and the issue has been properly identified and it can easily be remediated without risk of a data breach or theft of services.
  - The issue can be remediated within normal business hours.
  - The threat can be easily remediated by the state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.
- Special Events/Circumstances – A special event or circumstance incites hackers interested in trying to disrupt the agency’s IT services or cause

political embarrassment such as website defacements, and application hacking.

- Agency Impact – IT staff will take proactive measures, including applying patches, updating anti-virus files, and other system security measures, to address potential issue. Impact to IT services should be minimal since the threat has been identified and countermeasures exist for remediation.

7.2.4 Communication Procedures

A Level 2 - Medium situation means all IT resources are still operational. The following communication mediums will be utilized:

- Cybersecurity Portal – The CSO will use the cybersecurity portal to:
    - Post Information – The CSO will use the cybersecurity portal to post the current cybersecurity threat level and IT security information such alerts as the Microsoft and Linux Bulletins.
    - Incident Reports – ISOs and IT staff will use the portal to submit cyber related security information such as equipment theft, data breaches, and theft of services.
- Homeland Security Information Network (HSIN) Portal – The MC3 will use the HSIN Connect Room to:
    - Host public and private entities – During cyber centric events, the portal will be used to allow real-time communication and collaboration between participating organizations and individuals.
    - Communications may consist of – State updates, alerts, Indicators of Compromise (IOC), and outcomes.
- E-mail – E-mail will be used to provide alerts, status reports, updates, and ancillary information to critical infrastructure owners and operators.
- Telecommunications – Landlines and cell phones will be used for clarification purposes and to address questions about remediation efforts.

7.2.5 De-Escalation Criterion

To return to Level 1 - Low, the issue must be completely resolved and agencies must confirm IT resources are working normally and/or the special event has passed and additional security measures are no longer required.

7.2.6 Responsibilities

At this level the following groups will be active and perform assigned duties:

- Michigan Chief Information Officer (CIO) – The CSO will notify the CIO when an incident causes the state to escalate the cybersecurity threat level from Level 1 to Level 2. The CIO will work with agencies to make sure they comply with the remediation recommendations provided to them by the CSO and CTO.

- Michigan Chief Technology Officer (CTO) – The CTO will be responsible for communicating with the CIO. In addition to this, the CTO will ensure that all of the executive branch agencies assist with the remediation efforts.
- CSO – The CSO will work with the CIO and CTO to assist with communication and remediation efforts. The CSO will also coordinate any communications that need to occur between state agencies, the MS-ISAC, and the MI-ISAC. The CSO is responsible for notifying agencies when the alert level changes from Level 1 to Level 2. The CSO is also responsible for:
    - Incident Reports – The CSO will investigate incidents reported to them by ISOs, agency IT staff, or state employees.
    - Raising the Alert Level – The CSO will raise the alert level to Level 2 or Medium and notify the CIO’s Executive Management Team, Security Operations Section, EDC, and ISOs of the change and the reason for it.
    - Updating the Cybersecurity Portal – The CSO will change the level on the cybersecurity portal. The CSO in collaboration with the Public Information Officer (PIO) will provide local agencies and citizens with information about the threat and ways to avert it.
    - MI-ISAC Advisories – The CSO will work with the MI-ISAC to create advisories for distribution to ISAC members.
    - MS-ISAC Coordination – The CSO may need to contact MS-ISAC for more information about potential attacks or to request clarification on remediation efforts.
    - Remediation Efforts – The CSO assists agencies with remediating issues impacting their IT resources.
    - De-Escalation Process – The CSO will ensure that the issues that caused the alert level to be raised have been addressed before lowering the level back to Level 1.
    - MSP (EMHSD, MC3, MIOC) – The CSO will immediately contact the Michigan State Police (EMHSD, MC3, MIOC), by telephone and email, to apprise them of the situation and let them know if any assistance is needed. The MC3 and MIOC will coordinate with the National Guard via the Joint Operations Center to facilitate information sharing and resource preparedness.
    - State Security Operations Center (SOC) – The CSO will work with the SOC to identify and address potential cybersecurity incidents discovered by SOC security monitoring tools or reported by agencies, users, or citizens.
    - The CSO will identify and address potential cybersecurity incidents discovered by state agencies and functions or state government service providers. In addition to this, the CSO will be responsible for:

        - Incident Response – Investigating any cybersecurity related incidents reported to the SOC 24/7 Hotline.
        - Enterprise Firewall Management –Identifying and blocking IPs that attacks are originating from.
        - Remediation Effort – Designating team members to work with the CSO to remediate the issue(s).

- EDC – The EDC will work with the CSO to identify the appropriate actions necessary to remediate the threat. In addition to this, the EDC will be responsible for:
    - Security Monitoring Tools – The EDC will report any anomalies detected by security monitoring tools to the CSO.
    - Patch Management – The EDC will work with the CSO to identify the proper application patches and ensure they are installed on the servers that would be impacted by the threat. The inability to apply necessary patches will be documented. .
    - Antivirus – The EDC will ensure that all servers have the most current antivirus agents and files installed and that they are working correctly.
- Agencies – Agencies will work with their General Managers to address any concerns or issues; and to coordinate remediation efforts that may require assistance from the CSO or other agencies.
- ISOs – ISOs will help coordinate remediation efforts. In addition to this, ISOs will be responsible for:
    - Agency Alert Level – ISOs will be monitoring the incident and adjusting their agency alert level to properly match their readiness and remediation efforts.
    - Incident Reporting – ISOs are responsible for reporting incidents that may come about during remediation efforts or caused the agency to raise its alert level, to the CSO.
    - Communication – ISOs will work with the CSO, the EDC, Agency IT staff, and their customers to identify and communicate information about the incident and remediation efforts.
- Agency IT Staff – The agency IT staff will work with the ISOs, the CSO, and the EDC to identify and remediate issues impacting IT resources.
- State Government Service Providers (SPs) and other Business Partners (BPs) – SPs and BPs should reach out to their respective agency representatives to ensure they are aware of security (or threat) level changes and to take additional proactive measures to secure their IT infrastructure.
- MSP (EMHSD, MC3, MIOC) – MSP will monitor all resources, to determine if the threat is linked to cyber terrorist activities, and provide the CSO with information to help identify and mitigate the threat.

- MC3/MIOC – The MC3 and MIOC will work with the CSO and the FBI to identify potential threats that could impact the state and its business partners. The MC3 assists the CSO with events determined to be criminal in nature.
- MING – Will work with the MC3, MIOC and other partners to assist with the assessment of potential threats and information sharing when allowed by statute. The MING may be called upon to assist the CSO with the event if additional resources are required.

7.3 Cybersecurity Threat Level 3 - High (Orange)

Level 3 - High (Orange) is the third threat level in cybersecurity threat matrix. The following explains what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

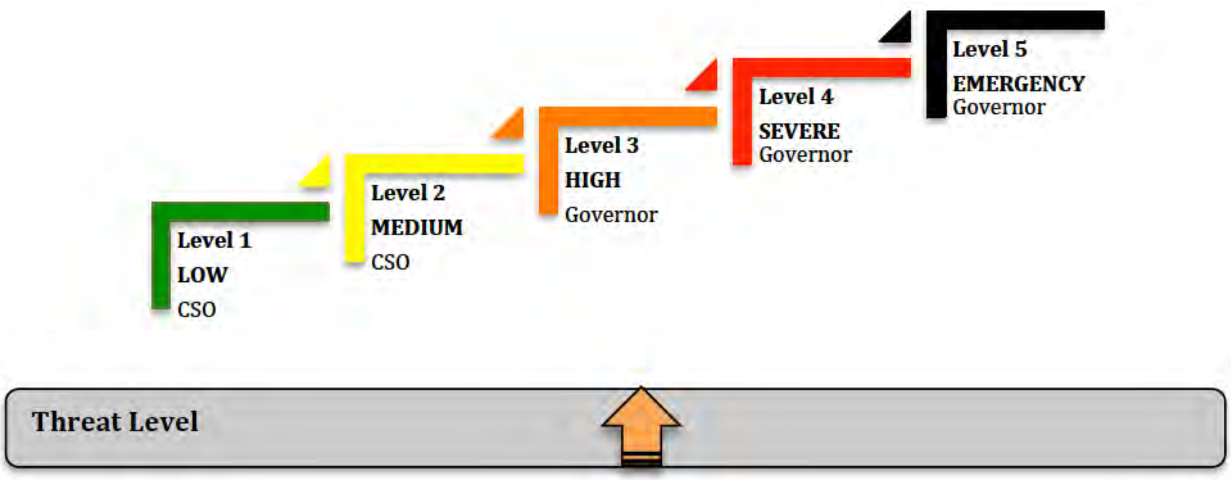


Figure 8: Level 3 – High (Orange)

7.3.1 Level Definition

Malicious activity has been identified in state networks with a moderate level of damage or disruption. Examples include but not limited to:

- An exploit for a vulnerability that has a moderate level of damage.
- Compromise of secure or critical system(s).
- Compromise of systems containing sensitive information or non-sensitive information.
- More than one agency affected in the state network with moderate level of impact.
- Infected by malware spreading quickly throughout the Internet with moderate impact.
- A distributed denial of service attack with moderate impact.

Actions:

- Continue recommended actions from previous levels.
- Identify vulnerable systems.
- Increase monitoring of critical systems.
- Contact MS-ISAC Security Operations Center (SOC) for additional guidance.
- Contact the MS-ISAC SOC for additional guidance. If APT is suspected request additional steps/procedures

- Immediately implement appropriate counter-measures to protect vulnerable critical systems.
- When available, test and implement patches, install anti-virus updates, and other system security measures as soon as possible.
- Contact the MC3 for awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes.
- Real time synchronous collaboration via phone and email as required. No financial considerations, no deployments, all activities conducted remotely. Consider SEOC activation and trigger point

7.3.2 Escalation

In order to raise the state or agency threat level to Level 3, the threat must involve two or more state agencies or critical infrastructure sectors (as defined in section 2.0), critical applications, or websites; and/or the risk of the threat has been determined to have a significant impact to state IT operations.

7.3.3 Potential Impact

At Level 3, the following conditions are in place:

- Impact to IT Services
  - A critical vulnerability, with the potential to cause significant damage if exploited, has been detected.
  - There are multiple web defacements.
  - A critical vulnerability is being exploited and there has been moderate impact.
  - Attackers have gained administrative privileges on compromised systems.
  - Critical applications or resources have been impacted.
  - Compromise of secure or critical system(s) containing sensitive information.
  - Compromise of critical system(s) containing non-sensitive information if appropriate.
  - IT Services may be interrupted by denial of service attacks.
  - The issue can be remediated within one to three business days and may require that critical application or services be taken offline until the issue can be remediated.
- The State Continuity of Operations Plan/Continuity of Government (COOP/COG) may have to be initiated to address the damages from the cyber-attack.
- Remediation Effort – The threat can be remediated by state agencies installing software patches, updating the antivirus files, or denying network access to specific IPs or IP ranges.

- Agency Impact
    - Agency IT staff will work with the CSO to install software patches, update antivirus files, or deny network access to specific IPs or IP ranges.
    - The CIO will work with the Governor's Office and Attorney General to address any political or legal ramifications that may arise from the incident.
- Cybersecurity Emergency Preparedness Liaison Officer (EPLO) will work with MSP/EMHSD to address any communication or facility needs the required by the agency to address the incident.

7.3.4 Communication Procedures

A Level 3 - High situation means that some of the state's IT critical resources have been impacted by a cybersecurity event or that multiple agencies have had significant security breaches. At this level, the following communication mediums will be utilized:

- MSP (EMHSD, MC3, MIOC) and MING – Will be notified by the CSO via email, telephone, cell phone or messenger and they will start making preparations to enact their internal cybersecurity emergency response plan.
- MS-ISAC – The CSO will notify MS-ISAC via a secure portal, e-mail, or telephone. The CSO may also request assistance from MS-ISAC with remediating the issue.
- MI-ISAC – The CSO will provide MI-ISAC members with updates or remediation information.
- Cybersecurity Portal – The CSO will continue to use cybersecurity portal to provide agencies and the citizenry with pertinent information.
- E-mail – E-mail will be used to communicate alerts, status reports, updates, and ancillary information.
- Telecommunications – Landlines and cell phones will be used for clarification purposes and to address questions about remediation efforts.

7.3.5 De-Escalation Criterion

To return to Level 2 - Medium, the incident must meet the criterion defined within that section and/or the special event has passed and additional security measures are no longer required.

7.3.6 Responsibilities

At this level the following groups will be active and perform assigned duties:

- CIO – The CIO will contact the Governor's Office to provide status updates. The CIO will also contact agencies to discuss potential contingency plans.
- CTO – The CTO works with the CIO and agencies to provide them with technical assistance in remediating the issues caused by incident(s).

- CSO – The CSO will work with the CTO and assist with communications identifying issues and remediation efforts. The CSO will brief MSP/EMHSD in time to prepare for setting up the SEOC. The CSO is also responsible for the following:
    - Incident Reports – The CSO will continue documenting and investigating incidents reported to them by ISOs, Agency IT staff, or state employees.
    - Raising the Alert Level – The CSO will raise the alert level to Level 3 or High and notify the CIO's Executive Management Team, EDC, and ISOs of the change and the reason for it.
    - Updating the Cybersecurity Portal – The CSO will change the level on the cybersecurity portal and collaborate with the Public Information Officer (PIO) to provide local agencies and citizens with information about the threat and ways to avert it.
    - MS-ISAC Notifications – The CSO will notify the MS-ISAC via secure portal, e-mail or telephone.
    - Increased Monitoring of Critical Systems - The CSO will monitor the state's critical systems to ensure the cybersecurity event is not affecting their operational status.
    - Remediation Efforts – The CSO will immediately implement appropriate counter-measures to protect vulnerable critical systems. The CSO will also continue recommended actions from previous levels and assist agencies with remediating the issues impacting IT resources.
    - De-Escalation Process – The CSO will ensure issues, that caused the alert level to be raised, have been addressed before lowering the level back to Level 2.
    - MSP (MC3, EMHSD, MIOC) Notifications – If this is a new event, the CSO will send MSP (MC3, EMHSD, MIOC) email notification appraising them of the situation and to let them know if any assistance is needed. If it is an escalated event, the CSO will let them know what happened to change the alert level.
- SP SOCs – SP SOCs will work with the CSO to identify and address potential cybersecurity incidents discovered by their security monitoring tools or reported to them by agencies, users, and citizens. Service Providers may also need to block IPs, DNS, and other potential attack vectors.
- The CSO will identify and block IPs that attacks are originating from and work with BPs to identify and remediate the issue(s).
- EDC – The EDC will work with the CSO to identify the appropriate actions necessary to remediate the threat. In addition to this, the EDC will address the following:

  - Security Monitoring Tools – The EDC will report any anomalies to the CSO.
  - Patch Management – The EDC will work with the CSO to identify the proper application patches and ensure they are installed on the servers that would be impacted by the threat.
  - Antivirus – The EDC will ensure all servers have the most current antivirus agents and files installed and are working correctly.
- ISOs – ISOs will help coordinate remediation efforts. In addition to this, ISOs will be responsible for:
  - Agency Alert Level – ISOs will monitor the incident and adjust their agency alert level to properly match their readiness and remediation efforts.
  - Incident Reporting – ISOs are responsible for reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
  - Communication – ISOs will work with agencies, the CSO, the CIO, Provider SOS, the EDC, Agency IT Staff, and their customers to identify and communicate information about the incident and remediation efforts.
- Agency IT Staff – The Agency IT Staff will work with the ISOs, CSO, and EDC to identify and remediate issues that are impacting IT resources.
- SPs and BPs – SPs and BPs should reach out to their respective agency representatives to find out if assistance is needed in the remediation effort.
- MIOC – The MIOC, in conjunction with the MC3, will reach out to federal and local contacts to apprise them of the situation and to determine if the event is isolated to the one particular state government or part of a larger attack being conducted by a nation state or cyber terroristic group.
- MC3 – The MC3 will determine if the event is criminal. In addition to the criminal investigation, the MC3 may be called upon to help the with the remediation effort.
- MING– Will work with the MC3, MIOC and other partners to assist as necessary. Michigan National Guard Cyber Teams (MI-NGCT) may be called upon to help with remediation efforts.

7.4 Cybersecurity Threat Level 4 - Severe (Red)

Level 4 - Severe (Red) signifies confirmed cyber-attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised state IT resources and are using them to propagate the attack or to spread misinformation. The following explains what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

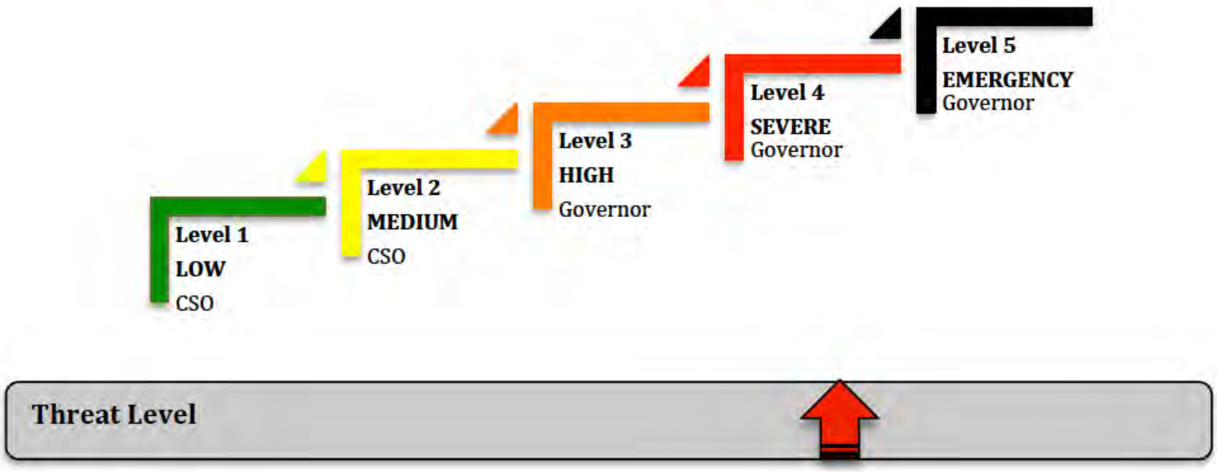


Figure 9: Level 4 – Severe (Red)

7.4.1 Level Definition

Malicious activity has been identified in state networks with a major level of damage or disruption. Examples include but are not limited to:

- Malicious activity impacting core infrastructure.
- A vulnerability is being exploited and there has been major impact.
- Data exposed with major impact.
- Multiple system compromises or compromises of critical infrastructure.
- Attackers have gained administrative privileges on compromised systems in multiple locations.
- Multiple damaging or disruptive malware infections.
- Mission critical application failures but no imminent impact on the health, safety or economic security of the state.
- A distributed denial of service attack with major impact.

Actions:

- Continue recommended actions from previous levels.
- Contact the MS-ISAC SOC for additional guidance. If APT is suspected request additional steps/procedures.

- Contact the MC3 for awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes. The MC3 will take enforcement actions through investigation and criminal prosecution.
- Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, and system log files for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Consider use of alternative methods of communication such as cellular phone, Voice Over Internet Protocol (VOIP), fax or state radio network in lieu of e-mail and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, and other measures immediately.
- SEOC activation based on conditions. Voluntary resource collaboration between members, technical information sharing & resource deployment based on mutual aid agreements. Could include financial considerations.

7.4.2 Escalation

To raise the state or agency threat level to Level 4, the threat must have the potential to impact multiple agencies and/or could require the state to shut down the IT infrastructure for five to ten business days to restore normal business operations.

7.4.3 Potential Impact

- Impact to IT Services
    - A critical vulnerability is being exploited and there has been significant impact.
    - Telecommunications may be interrupted causing agencies to use alternate forms of communication.
    - E-mail communications may be disrupted or untrusted making it necessary for agencies impacted by the event to use alternate forms of communication.
    - CIO Executive Management Team may have to be relocated to the SEOC for command and control purposes.
    - Agency IT Operations may have to be relocated to the SEOC for command and control purposes.
    - COOP may have to be implemented to restore IT operations.
    - Normal grid supplied power may become unreliable/unavailable for extended periods of time and considerations of emergency backup power are being prioritized.

  - Multiple damaging or disruptive virus attacks; and/or, multiple denial of service attacks against critical infrastructure services.
  - The issue can be remediated within five – ten business days and may require critical applications or services be taken offline until the issue can be remediated.
  - The COOP/COG will need to be initiated to address the damages from the cyber-attack.
  - The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems, or applications to a previous date before the attacks occurred.
- Agency Impact
  - Agency IT staff will work with the CIO to restore their equipment, systems, and applications to an operational state.
  - Agencies will work with the, Governor's Office and Attorney General to address any political or legal ramifications that may arise from the incident.
  - Cybersecurity EPLO may need to relocate to the SEOC and work with CIO and agency IT staff to restore IT Operations.

7.4.4 Communication Procedures

At Level 4 - Severe, the state's IT critical resources have been severely impacted by a cybersecurity event that has caused IT service to be offline/unreliable for an extended period of time. This event may be impacting telecommunications and may cause incident responders to use alternate forms of communications.

- MSP/EMHSD – MSP/EMHSD will be notified via email (if available), telephone, cell phone or messenger and they will start making preparations to enact their internal cybersecurity emergency response plan. In addition to this, MSP/EMHSD will:
  - Provide executive conference rooms for the CIO, CTO, CSO and agencies, to assist with the recovery process.
  - Provide operational conference rooms for EPLOs and agency IT staff assisting with restoring telecommunications.
  - Establish temporary communications (radio, messengers, etc.) for recovery personnel.
  - Notify the MING JOC via email (if available), telephone, cell phone or messenger.
  - Issue radios to first responders assisting in the recovery process.
- MS-ISAC – The CSO will contact the MS-ISAC via email (if available) or telephone and if necessary request assistance with remediating the issue.

- MI-ISAC – The CSO will provide MI-ISAC members with an update or share remediation data.
- Cybersecurity Portal – The CSO will continue to use cybersecurity portal to provide agencies and the citizenry with pertinent information.
- E-mail – If available, e-mail will be used to communicate alerts, status reports, updates, and ancillary information.
- Telecommunications – Telecommunications may become unreliable making it necessary for first responders to use alternate forms of communication
- Messengers – Depending on the nature of the event, the state may have to use messengers to communicate information between incident responders and the CIO and MC3.

7.4.5 De-Escalation Criterion

To return to Level 3 - High, the incident must meet the escalation criterion identified within that section and/or the special event has passed and additional security measures are no longer required.

7.4.6 Responsibilities

At this level the following groups will be active and perform assigned duties:

- The CIO – The CIO will contact the Office of the Governor report on the severity of the situation. In addition to this, the CIO will:
  - Determine if COOP should be activated.
  - Determine if the CIO should relocate its IT administration to the SEOC for command, control, and communication purposes.
  - Review contingency plans.
  - Assist the Governor and cabinet members with:
    - Crafting sensitive communications to politicians, media, and other parties as required.
    - Contacting the State Budget Office (SBO) to obtain emergency funding to replace equipment and resources damaged or destroyed by the event
- CTO – The CTO will:
  - Work with the CIO and agency IT staff to coordinate the recovery process and to provide technical assistance in remediating the issues caused by incident(s).
  - Identify critical assets that have been damaged or destroyed by the incident and forward the information to the CIO to request emergency purchase.
  - Ensure the COOP Incident Command Team is contacted and briefed.
  - Ensure agency directors are briefed and begin making preparations to assist the COOP Incident Command Team.

  - Ensure the COOP alternate facilities are prepped.
  - Ensure that alternate communications are in place and operational.
  - Establish networks and communication to alternate facilities that
- CSO – The CSO will assist the CIO and CTO with communications that identify the issues and remediation efforts. The CSO is responsible for notifying agencies when the alert level changes from Level 3 to Level 4. In addition to this, the CSO will:
  - Incident Reports – The CSO will continue documenting and investigating incidents reported to them by ISOs, Agency IT staff, or state employees.
  - Raising the Alert Level – The CSO will raise the alert level to Level 4 and notify the CIO's Executive Management Team, Provider SOS, EDC, agency IT staff, and ISOs of the change and the reason for it.
  - Updating the Cybersecurity Portal – The CSO will change the level on the cybersecurity portal and provide local agencies and citizens with information about the threat and ways to avert it.
  - Remediation Efforts – The CSO will:
    - Continue recommended actions from previous levels.
    - Assist agencies with remediating the issues that are impacting their IT resources.
    - Assist MSP/EMHSD is establishing alternate forms of communication.
    - Closely monitor security mechanisms, including firewalls, web log files, anti-virus gateways and system log files, for unusual activity.
    - Consider limiting or shutting down less critical connections to external networks such as the Internet.
    - Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- The CSO will ensure issues that caused the alert level to be raised have been addressed before lowering the level back to Level 3.
- Telecommunications Service Provider SOC – The Telecommunications Service Provider will work with the CSO to help identify issues, block firewall ports, and assist with remediation efforts. The Telecommunications Service Provider may also be called upon to work with the CSO to reroute network traffic to systems that are not impacted by the cyber-attack.
- The CSO will identify and address potential cybersecurity incidents discovered by security monitoring tools or reported to them by agencies, users and citizens. In addition to this, the CSO will direct:
  - Incident Response – the CSO will forward any cybersecurity related incidents reported to the SOC 24/7 Hotline.

  - Enterprise Firewall Management – the CSO will identify and block IPs that are the origin of attacks.
  - Remediation Effort – the CIO will designate team members to work with the CSO to remediate the issue(s).
- The EDC – The EDC will work with the CSO to identify the appropriate actions necessary to remediate the threat. In addition to this, the EDC will:
  - Security Monitoring Tools – The EDC will report any anomalies to the CSO.
  - Patch Management – The EDC will work with the CSO to identify the proper application patches and ensure they are installed on servers that would be impacted by the threat.
  - Antivirus – The EDC will ensure that all servers have the most current antivirus agents and files installed and working correctly.
- ISOs – ISOs will help coordinate remediation efforts within their respective agencies. In addition to this, ISOs will be responsible for:
  - Agency Alert Level – ISOs will be monitoring the incident and adjusting their agency alert level to properly match their readiness and remediation efforts.
  - Incident Reporting – ISOs are responsible for reporting any incident that may come about during the remediation efforts or that may have caused the agency to raise its alert level.
  - Communication – ISOs will work with the CSO, CIO, EDC, Agency IT Staff, and their customers to identify and communicate information about the incident and remediation efforts.
- Agency IT Staff – The Agency IT Staff will work with the ISOs, CSO, CIO, and EDC to identify and remediate issues impacting IT resources.
- BPs and SPs – BPs and SPs should reach out to their respective agency representatives to find out if assistance is needed in the remediation effort.
- MSP/EMHSD – MSP/EMHSD will reach out to federal and local contacts to apprise them of the situation and to determine if the event is isolated to the state or part of a larger attack being conducted by a nation state or cyber terroristic group.
- MC3/MIOC – The MIOC will work with law enforcement and Department of Homeland Security (DHS) to determine if the event is criminal. In addition to the criminal investigation, MC3 may be called upon to help with the remediation effort.
- MING – Will work with MC3/MIOC and other state and federal partners to assist as necessary. MING JOC may begin recall of Cyber Mission Forces as directed by the Adjutant General or other designated MING official. MI-NGCT may be called upon to assist with remediation efforts.

7.5 Cybersecurity Threat Level 5 - Emergency (Black)

At Level 5 – Emergency (Black), unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks have an impact at the national, state, and local level. The following explains what this level means and the impact it has on state agencies, business partners, local governments, and citizens.

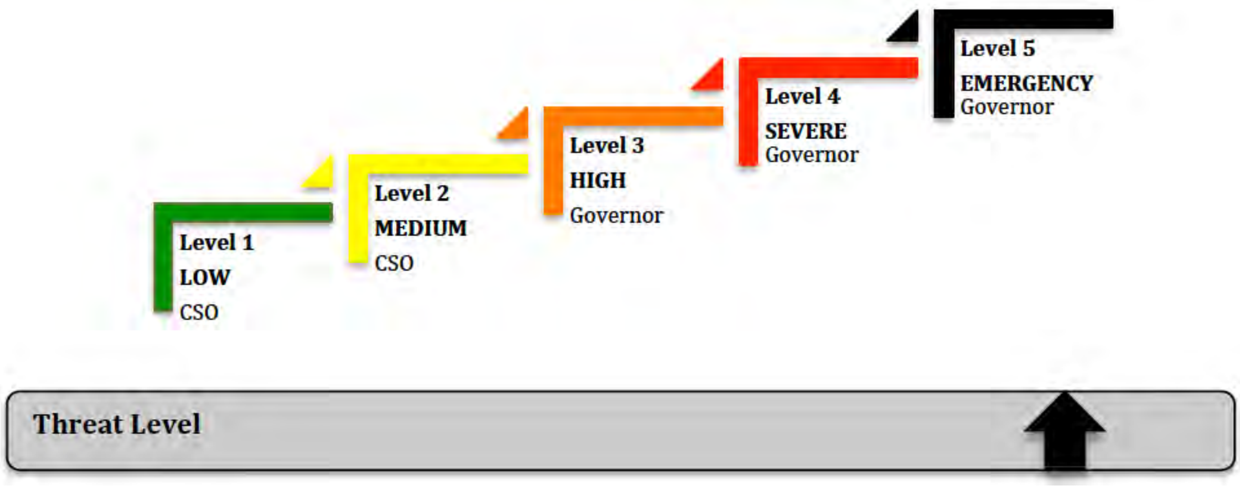


Figure 10: Level 5 – Emergency (Black)

7.5.1 Level Definition

Malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but are not limited to:

- Malicious activity results in widespread outages and/or complete network failures.
- Data exposure with severe impact.
- Significantly destructive compromises to systems, or disruptive activity with no known remedy.
- Mission critical application failures with imminent or demonstrated impact on the health, safety or economic security of the state.
- Compromise or loss of administrative controls of critical system.
- Loss of critical Supervisory Control and Data Acquisition (SCADA) systems.

Actions:

- Continue recommended actions from previous levels.
- Contact the MS-ISAC SOC for additional guidance. If APT is suspected request additional steps/procedures.
- Activate the Michigan Cyber Civilian Corps (MiC3) to support response activities.

- Contact the MC3 for awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes. The MC3 will take enforcement actions through investigation and criminal prosecution.
- Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternate methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.

7.5.2 Escalation

To raise the state or agency threat level to Level 5, the following conditions must be in place:

Risk Level – The threat has impacted multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.

7.5.3 Potential Impact

- Impact to IT Services
  - Telecommunications are unavailable making it necessary to use alternate forms of communication.
  - The power grid is unreliable causing agencies to rely on backup generators or uninterrupted power supply (UPS).
  - Buildings have been damaged or destroyed rendering IT resources inoperable.
  - CIO’s Executive Management Team has to relocate to the SEOC for command and control purposes.
  - COOP has to be implemented to restore IT operations.
  - Datacenters have to be restored or relocated to alternate facilities.
  - The issues will take over six business days to remediate and critical applications and services will be offline until the issues can be remediated.
  - The threat can only be remediated by restoring the applications, systems, and facilities to an operational state by rebuilding equipment or restoring critical systems or applications to a previous date before the attacks occurred.
- Agency Impact
  - Agency IT staff will work with CIO to restore equipment, systems, and applications to an operational state.

    - The CIO will work with the Governor's Office and Attorney General to address any political or legal ramifications that may arise from the incident.
    - Cybersecurity EPLO may need to relocate to the SEOC and work with CIO and their agency IT staff to restore IT Operations.

7.5.4 Communication Procedures

At Level 5 - Emergency the state's critical IT resources are rendered inoperable by a cybersecurity attack that will take weeks to recover. Such an event will impact IT communications and necessitates the need for alternate forms of communications (satellite, radios, messengers, etc.).

- SEOC – The SEOC will be notified via cell phone or messenger and they will enact their internal cybersecurity emergency response plan. In addition to this, the SEOC will:
    - Provide executive meeting and conference rooms for the CIO and CTO to assist with the recovery process.
    - Establish temporary communications (radio, satellite, etc.) for recovery personnel.
    - Provide operational meeting and conference rooms for EPLOs and Agency IT staff assisting with restoring telecommunications.
- MS-ISAC – The CSO will contact MS-ISAC via email (after email communications is restored) or telephone and request assistance with remediating the issue.
- MI-ISAC – After email communication is restored, the CSO will use email to provide MI-ISAC members with an update or to share remediation data.
- Cybersecurity Portal – Once the state's network is restored, the CSO will use the cybersecurity portal to provide agencies and the citizenry with pertinent information.
- E-mail – When restored, e-mail will be used to communicate alerts, status reports, updates, and ancillary information.
- Telecommunications – After telecommunications are restored, land lines and cell phones will be used for clarification purposes and to address questions about remediation efforts.

7.5.5 De-Escalation Criterion

To return to Level 4 - Severe, the incident must meet the escalation criterion identified within that section and/or the special event has passed and additional security measures are no longer required.

7.5.6 Responsibilities

When the state is at this level the following groups will be active and carry out their assigned duties:

- CIO – The CIO will contact the Governor's Office to report on the severity of the situation. The CIO will also:
    - Activate the COOP.
    - Relocate appropriate Governor's Office staff to the SEOC, Alternate SEOC (ASEOC) for command, control, and communication purposes.
    - Review contingency plans.
    - Assist the Governor's Office and MSP/EMHSD with crafting sensitive communications to politicians, media, etc.
    - Assist the Governor's Office with contacting SBO to coordinate emergency funding to replace equipment and resources damaged or destroyed by the event.
    - Work with DTMB to acquire alternate work sites for employees with offices in buildings and structures damaged or destroyed by the incident.

- CTO – The CTO will be responsible for:
    - Working with the CIO, agency IT staff, and the Deputy State Director of Emergency Management and Homeland Security to coordinate the recovery process and to provide technical assistance in remediating the issues caused by the incident(s).
    - Identifying critical assets that have been damaged or destroyed by the incident and forwarding the information onto the CIO to request emergency purchase.
    - Ensuring that COOP Incident Command Team is contacted and briefed.
    - Ensuring that Agency Directors are briefed and they start making preparations to assist the COOP Incident Command Team.
    - Ensuring COOP alternate facilities are prepped.
    - Ensuring alternate communications are in place and operational.
    - Establishing networks and telecommunications to Governor's Office and state agency alternate facilities.
- CSO – The CSO will activate the MiC3 and work with the CTO to assist with communications, identifying issues and remediation efforts. At this level, the CSO is responsible for:
    - Incident Reports – The CSO is responsible for documenting what occurred and providing the CTO with a post mortem report.
    - Raising the Alert Level – The CSO will raise the alert level to Level 5 and notify the CIO's Executive Management Team, EDC, agency IT staff, and ISOs of the change and the reason for it.

      Note: This may require the information to be communicated via a courier or a messenger service.

    - Updating the cybersecurity portal – If the portal is available, the CSO will change the level on the cybersecurity portal and use it to convey critical information.
    - Remediation Efforts – The CSO will:
        - Continue recommended actions from previous levels.
        - Assist agencies with remediating the issues that are impacting IT resources.
        - Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
        - Isolate internal networks to contain or limit damage or disruption.
        - Use alternate methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.
    - De-Escalation Process – The CSO will ensure issues that caused the alert level to be raised have been addressed before lowering the level back to Level 4.
- Service Providers SOC – The Service Provider SOC will participate on any conference calls that the CSO sets up. In addition to this, they will advise the CSO of any information from its business partners that could help restore the state's infrastructure.
- EDC – The EDC will work with the CSO to identify necessary actions needed to remediate the threat.
- ISOs – ISOs will work with their agency IT staff to help coordinate remediation efforts, and are responsible for reporting any incidents that may occur during remediation efforts or that may have caused the agency to raise its alert level.
- Agency IT Staff – The Agency IT staff will work with the ISOs, CSO and EDC to identify and remediate issues impacting IT resources. Agency IT staff may need to activate their disaster recovery plan.
- BPs – BPs should reach out to their respective agency representatives to find out if assistance is needed with the remediation effort.
- MSP/EMHSD – The Director of MSP/EMHSD will join the CIO, CTO, and critical infrastructure agency CIOs at the SEOC or a designated recovery site. During SEOC activation, MSP/EMHSD will maintain communications with federal and local contacts to apprise them of the situation and receive any information DHS may have about the event.
- MC3/MIOC – The MC3 Commander and MIOC Director will join the CSO staff at the SEOC or a designated recovery site to help restore the state's critical infrastructure. The MC3 will determine if the event warrants

investigation for potential criminal activities. The MIOC will work with local authorities to advise/assist them with the recovery process.

- MING – The MING Cyber Operations Officer or Senior Cyber representative will join the staff at the SEOC or designated recovery site to help restore the state's critical infrastructure as directed by the Governor. MI-NGCT members will be activated as required to support operations.
- MiC3 – MiC3 volunteers will report to CSO designated IT and EM functions to support response and remediation efforts.

8.0 Plan Maintenance

The State of Michigan Chief Security Officer (CSO) and Department of Technology, Management and Budget (DTMB**)** are responsible for overall administration and maintenance of this plan and monitoring and reporting on its progress. This process includes periodic reviews as well as updates to incorporate changes achieved through the completion of planned initiatives and lessons learned from exercises and real-world situations.

9.0 Authorities and References

- Presidential Policy Directive-21: Critical Infrastructure Security and Resilience
- Department of Homeland Security National Infrastructure Protection Plan 2013 (NIPP): Partnering for Critical Infrastructure Security and Resilience
- Homeland Security Presidential Directive-5 (HSPD-5): Management of Domestic Incidents
- Homeland Security Presidential Directive-7 (HSPD-7): Critical Infrastructure Identification, Prioritization and Protection
- Homeland Security Exercise and Evaluation Program (HSEEP)
- NIST Special Publication 800-55 Revision 1, Security Measurement
- NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide

This page intentionally left blank

Annex A: Communication

A.1 Introduction

This annex provides the operational guidelines for developing and implementing the protocol to support communication among members and stakeholders to mitigate the effects of cyber disruption.

A.2 Roles & Responsibilities

Michigan State Police is responsible for statewide emergency management, homeland security, coordination of Michigan critical infrastructure protection, and consideration for criminal investigation and prosecution.

Critical Infrastructure Owners and Operators provide, maintain and operate assets and resources critical to sustaining public and private entity operations and the health and welfare of individual citizens.

Public and Private Partners include local government agencies, non-governmental organizations (NGOs) and private entities that are key partners but not part of the critical infrastructure.

Authorized Agents are formally authorized by strategic partnership entities to use this protocol. Partners will provide the name, title, primary and alternate phone numbers, and email addresses of Authorized Agents. The rotational chairperson will maintain an updated list and provide a current copy to the State of Michigan CSO and the MC3. Upon receipt of the list, the MC3 will contact each Authorized Agent to request a unique passphrase for validation purposes. This passphrase will be documented in the listing maintained in the MC3.

A.3 Activation Parameters

The Michigan Cyber Disruption Response Strategy Communication Protocol will be activated when:

1. A cooperating member of the strategic partnership has experienced, or is experiencing, a harmful cyber disruption due to a novel cyber anomaly and has a demonstrated need to issue a warning or request assistance; or,
2. A cooperating member would like to share important information regarding emergent cyber anomalies or threats.

A.4 Authorized Agents

The information owner will classify notifications issued by authorized agents according to one of the following classifications:

1. **Confidential** – Authorized Agents Only.
2. **Proprietary** – Share within the member community only.
3. **Public** – Available for public disclosure.

Information shared within the partnership shall remain the property of the information owner, and shall therefore not be reclassified by anyone other than the owner.

Due to governmental involvement in the Michigan Cyber Disruption Response Plan, documentation pertaining to activities undertaken by the strategic partnership could be subject to Freedom of Information Act (FOIA) requests. As such, all FOIA requests should be forwarded to the State of Michigan for review by state FOIA coordinators to ensure compliance with applicable laws.

A.5 Communication Protocol

A.5.1 Description

The MC3 will determine the means of disseminating reports based on the assigned Action Level and Notification Type:

Action Level	Notification Type	Protocol
1	Emergency	SMS/Text/MSP/Email, Phone Call, Conference Line
2	Important Notification	SMS/Text/MSP/Email, Automated Phone Call
3	For Information Only	SMS/Text Message/Email

Table A-1: Communication Protocol Description

A.5.2 Activation Steps

To activate the Communication Protocol:

1. An Authorized Agent initiates communication by calling the MC3 at *877-MI-CYBER (877-642-9237) or 517-241-8000.*
2. The officer verifies the Authorized Agent using an authorization list and unique passphrase.
3. The Authorized Agent reports the details outlined in Figure 3.
4. The MC3 will:
    a. Determine the Action Level and implement the corresponding Communication Protocol.
    b. Log all relevant information.
    c. Complete all after action reporting tasks.

CDRT activation can be authorized by the CDRT chairperson or vice chairperson upon request by CDRT member organizations or the Michigan EM team. Activation decisions are made based upon the trigger criteria described below.

A.5.3 Activation Triggers

Activation of the CDRT may result from:

- Major disruptions of power grids in the region
- Threat to or widespread loss of communications and data networks (e.g. internet, mobile/cellular)
- Imminent threats to critical government facilities

- Significant cyber incidents
- Physical damage to a critical cyber asset
- Loss of access to a facility hosting a critical cyber asset
- Loss of staff (e.g., injury, sickness, or death) with irreplaceable knowledge of critical cyber systems

A.5.4 Activation Process

The initiating chairperson will notify appropriate CDRT members of a meeting or conference call by means of email, telephone, radio, satellite phone, or messenger.

The Cyber Disruption Incident Report Form (Figure A-3) will be completed by the agency that initiates the meeting/call and will be distributed prior to the meeting/call.

The CDRT Meeting/Call Agenda (Figure A-4) outlines discussion topics.

The chairperson initiating the call will appoint a recorder to document issues discussed using the CDRT Meeting/Call Note-taking Template (Figure A-5).

A.6 CDRT Communications

A.6.1 CDRT Activation Notification

When the CDRT chair decides to initiate a CDRT meeting or teleconference, the initiator develops a brief message indicating the date, time, who is activated, communication method (e.g., teleconference, in-person), and summary of the reason for the activation:

"CDRT Activation in response to Detroit-area major power outage. CDRT Core and Associate Members. Teleconference scheduled for 7/10/2015 at 1300 on 888-555-1212 x123456. If communication systems fail, Core members will meet at Lansing JOC at 442 Roper Ave at 1400."

The primary contact method for internal CDRT notifications is the SendWordNow notification service. This service delivers messages to registered users via email, text, and telephone, based on the contact information provided by the user. SendWordNow includes an acknowledgement function to notify the sender when a message has been received.

Secondary contact method is direct telephone and text messaging to both primary and secondary landline and cellular phone numbers provided by the CDRT member.

Tertiary contact method is direct telephone contact to the CDRT members' place of business, home, and in-case-of-emergency contact numbers to leverage work and home contacts to relay a message or ascertain location and status.

The final contact method is physical notification and retrieval of the CDRT members from their locations.

A.6.2 Post-activation Communications

Following the first CDRT meeting/call, CDRT members may be deployed to various locations to assist in the response. It is critical that CDRT members are reachable during a disruption event, particularly as it is unfolding.

After initial activation, each CDRT meeting should conclude with the date; time; location; and primary, secondary, and alternate communication provisions for the next meeting. The time and location of a physical meeting 1–2 hours following the next regularly scheduled teleconference will also be provided in case traditional communication methods are inoperable.

Information about the next meeting will also be communicated to the relevant CDRT members per the initial activation procedures described above.

A.6.3 External CDRT Communications

The CDRT Chair/ Vice-Chair or CDRT member authorized to act on behalf of the CDRT, such as a public information officer, must approve all official CDRT communications.

A.6.4 Multi-Jurisdictional CDRT Communications

The CDRT chairperson will use discretion to determine whether a regional or multi-jurisdictional communication system is necessary.

Coordination for planning, situational awareness, and response activities may be achieved through the following process:

- The CDRT chairperson or their designee may initiate communication between multiple state CDRTs.
    - It is recommended that jurisdiction hierarchy (e.g., city, county, region, state, or federal) be recognized and respected, when appropriate.
- The initiating chairperson will send notifications to the appropriate CDRT members and/or chairpersons of other state or jurisdictional CDRTs to participate in a conference call by means of email, telephone, radio, satellite phone, or messenger.
- The Cyber Disruption Incident Report Form (Figure A-3) will be completed by the initiating agency and distributed prior to the scheduled call.

All notified CDRT chairpersons and appropriate stakeholders will call the phone or radio bridge detailed in the call invitation as scheduled. The initiating chairperson will provide objectives of the communications, and any call or other contact information necessary to participate on a communication.

- The initiating chairperson will be the communication’s facilitator.
- The initiating chairperson will provide a recorder to document meeting details using the call agenda and note-taking template (Figure A-5).

- CDRT plans developed during meeting sessions will be documented on the Incident Action Plan Form (Figure A-2).
- The recorder should provide notes to all participants within one hour via email or fax. If these methods of communication are not available, it is recommended that each participating organization provide a recorder.

Cyber Disruption Response Team Contact List

Organization	Contact / Position	Contact Information
State of Michigan	CIO	
State of Michigan	CTO	
State of Michigan	CSO	
Organization/ Department 4		
Organization/ Department 5		

Figure A-1: CDRT Contact List

CDRT Incident Action Plan

Incident:	**Date:** ____________________ **Time:** ____________________
1. Call Participants (including backup means of communication for each participant)	
2. Situation Status	
5. Current Issues	

Incident:	**Date:** ____________________ **Time:** ____________________
6. Actions, Strategies, and Tactics (including responsible parties, timeframes for actions, etc.)	
7. Required Resources	
8. Approved By (Name and Position)	

Figure A-2: CDRT Incident Action Plan (IAP)

Cyber Disruption Incident Report Form

Prepared by: ______________________________ Contact Email: ____________________________ Contact Phone: ___________________________ Emer. Contact: ____________________________	Date: _____________ Time: _______________ Incident Location: __________________________ Street Address: _____________________________ _______________________________________
Critical Assets Affected: ______________________ ____ ____	Facility Points of Contact: __________________ _______________________________________ _______________________________________
Type of Incident: ____ Incident Summary: ____ ____ ____ Means of Detection: ____ ____ ____	
Business Process Affected: ____ ____	
Preparer’s Signature: _______________________	Manager Signature: _______________________

Figure A-3: Cyber Disruption Incident Report Form

CDRT Meeting/Call Agenda

Task	Responsible Party	Resources
1. Call meeting/teleconference to order	Meeting/Call organizer	Standard meeting/call agenda
2. Assign recorder	Meeting/Call organizer	Standard meeting/call note-taking template
3. Introductions	Participants	
4. Overall situation briefing	Meeting/Call organizer	CDRT IAP (if completed) and/or cyber disruption incident reporting form
5. Organizational situation briefings Include actions from last operational period	Representatives (two minutes max per briefing)	Cyber disruption incident reporting form
6. Additional situational awareness info	All/Any call participants	
7. Critical issues	Organizational representatives	CDRT IAP (work through IAP from previous Operational Period (OP) and create new IAP for next OP)
8. Critical issue recap	Meeting/Call organizer	CDRT IAP (work through IAP from previous OP and create new IAP for next OP)
9. Duration of next OP	Meeting/Call organizer	CDRT IAP (create new IAP for upcoming OP)
10. Immediate next actions and required resources within OP	Organizational representatives	CDRT IAP (create new IAP for upcoming OP)
11. Immediate actions, tasks, and resources recap	Meeting/Call organizer	CDRT IAP (create new IAP for upcoming OP)
12. Mid-/long-term goals and required resources	Organizational representatives	CDRT IAP (create new IAP for upcoming OP)
13. Unresolved issues	Meeting/Call organizer	
14. Schedule next call/meeting, date, time, and place	Meeting/Call organizer	CDRT IAP (create new IAP for upcoming OP)

Figure A-4: CDRT Meeting/Call Agenda

CDRT Meeting/Call Note-taking Template

1. Call Meeting to Order: Meeting/Call Organizer

Date:

Start Time:

Location:

2. Participants:

Name Organization Contact Phone

3. Situation Briefing: Meeting/Call Organizer

4. Organization Situation Briefings: Organization Representatives

Include Actions from Last Operational Period

Organization ________________– Situation Briefing:

Organization ________________– Situation Briefing:

Organization ________________– Situation Briefing:

Organization ________________– Situation Briefing:

5. Additional Situational Awareness Info: All/Any Call Participants

Participant: ________________

Issue:

Participant: ________________

Issue:

Participant: ________________

Issue:

Participant: ________________

Issue:

Participant: ________________

Issue:

6. Critical Issues: Organization Representatives

Organization ________________– Critical Issues:

Organization ________________– Critical Issues:

Organization ________________– Critical Issues:

Organization ________________– Critical Issues:

Organization ________________– Critical Issues:

7. Critical Issue Recap: Meeting/Call Organizer

8. Next Operational Period (OP): Meeting/Call Organizer

9. Immediate Next Actions and Required Resources within OP:

Organization Representatives

Organization ________________

Immediate Next Action:

Resources Required:

Organization ________________

Immediate Next Action:

Resources Required:

Organization ________________

Immediate Next Action:

Resources Required:

Organization ________________

Immediate Next Action:

Resources Required:

Organization ________________

Immediate Next Action:

Resources Required:

10. Immediate Actions, Tasks, and Resources Recap: Meeting/Call Organizer

11. Mid- and Long-Term Goals and Required Resources: Organization Representatives

Organization ________________

Mid-/Long-Term Goals:

Resources Needed:

Organization ________________

Mid-/Long-Term Goals:

Resources Needed:

Organization ________________

Mid-/Long-Term Goals:

Resources Needed:

12. Any Unresolved Issues: Meeting/Call Organizer

13. Next Call: Call Organizer Meeting Date: Time and Place:
14. Meeting Adjourned: Call Organizer Time of Adjournment:

Figured A-5: CDRT Meeting/Call Note-taking Template

Michigan CDRT Members

CDRT Chair(s) and/or Vice Chair:	[Emergency management agency, law enforcement, and/or IT representative]
Participating Agencies:	Department of Technology Management & Budget Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD) [Law Enforcement – Local, County, and State] Michigan State Police, Michigan Cyber Command Center (MC3) Michigan State Police, Michigan Intelligence Operations Center (MIOC) Michigan National Guard [Public Safety] [Private Sector] [Others as determined necessary]
Regional and National Contacts:	United States Computer Readiness Team (US-CERT) Multi-State Information Sharing Analysis Center (MS-ISAC) DHS/FEMA Region V [Other regional and National contacts]
Private Contacts:	[Private telecom representative] [Power company representative] [Others private contact]

Annex B: Response Plans

B.1 Introduction

This annex provides a template for the development of cyber response plans for Michigan's critical infrastructure, and a framework for response to cyber disruptions. These efforts are based on the cyber incident response cycle, which describes the "fundamental elements of prevention and protection activities" associated with a cyber-response.

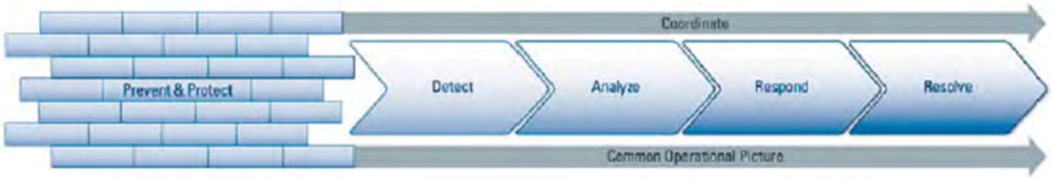


Figure B-1: Interim National Cyber Incident Response Plan Incident Response Cycle

B.2 Response Plan Template

B.2.1 Introduction

Incident response plans provides a set of instructions for critical infrastructure owner and operator cyber security incident response team execution in the event of a given security incident. Each response plan is effectively a Play Book used to prevent uncoordinated responses to potentially devastating security incidents.

B.2.2 Background

To ensure consistency of approach across all departments it is essential that they are use the same basic framework as outline in the proposed template. The benefit of this is that if a responder moves to a different team, there will be a very small learning curve to get up to full speed.

B.2.3 Critical Systems Information

Critical systems, applications and services should be properly identified, included in the asset management system and recovery and restoration directions must be clearly defined. At a minimum, the following information should be maintained for each critical system:

- System Name
- Classification
- Location
- Owner
- Restoration Priority
- Configuration Information
    - Build
    - Patch
- Location of Backup

- Restoration Checklist
- Subject Matter Expert

B.2.4 Concept of Operations

Organizations should develop a Concept of Operation (ConOps), which is a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint. The ConOps describes the user organization (mission(s) and organizational objectives from an integrated systems point of view. This section defines what the organizations Incident Response Plan is; how it affects the user; why it is vital and what users need to know/do.

a) Prevention and Protection

- Prevention
    - Incident Handler
        - Communications
        - Facility (e.g., In-House or Contract)
    - Incident Analysis Hardware & Software
    - Incident Analysis Resources
    - Incident Mitigation Software
- Protection
    - Risk Assessments
    - Host Security
    - Network Security
    - Malware Prevention
    - User Awareness & Training
    - Patch Management

b) Detection and Analysis

- Log Management and Alert Integration
- Security Event Triage Processing
- Security Event Validation
- Event Analysis and Possible Escalation to Security Incident

c) Response and Recovery

- Response Plan Activation
    - Security Event Escalation
    - Response Team Call-out Tree Activation
    - War Room Invocation
    - Extended Response Team Activation
- Response Activities
    - Communications Lockdown for Serious Events
    - Further Event Analysis and Response Selection from Response Play Book
    - Response Playbook Execution and Results Documentation
        - Affected Systems Containment
        - Known Threat Blockage

- Implementation of Additional Controls to Stop Threat
- Damage Identification
- Damage Eradication and Identification of Required Restoration

B.2.5 Specific Cyber Response Action Plans

a) Data Backup Action Plan

- Identification of Data to Be Backed Up
    - Network Servers
    - Desktop Computers
    - Laptop Computers
    - Wireless Devices
    - Network Devices
    - Security Devices
- Backup of Vital Hard Copy Records
- Backup Software & Hardware
- Backup Media
    - Location
    - Classification
- Storage
    - In-House
    - Cloud
- Restoration
    - Test/Validation

b) Disaster Recovery/Business Continuity Plan (DR/BCP)

This plan covers recovery strategies for Information Technology (IT) systems, applications and data, including networks, servers, desktops, laptops, wireless devices, data and connectivity. IT recovery priorities should be consistent with the priorities for recovery of business functions and processes developed during the Business Impact Assessment (BIA). IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective (RTO) for the business function or process that depends on the IT resource. The following are standalone plans referenced by the DR/BCP plan, which could place them as outlines in separate annexes:

c) Halt Key Processes Plan

- Identifies and documents key processes.
- Describes the order and any dependencies that affect how these processes should be safely and completely halted.
- Roles and responsibilities for achieving these shutdowns must also be documented.

d) Equipment Shutdown Plan

- Identifies and documents key items of equipment or plant that require specific and detailed shutdown processes.
- Describes the order and any dependencies that affect how these items of equipment should be safely and completely shut down and the processes needed to implement this.
- Roles and responsibilities for achieving these shutdowns must also be documented.

e) Log File Recovery Plan

- Defines processes to synchronized log file data from remote locations.
- Provides test plan to validate this process operates correctly.

f) Communication Plan (Include Media, Executives, etc.)
Include directions on:

- Secure Communications Channels
- Incident Communications
  - Team Notifications
  - Incident Updates
- Communications Types/Updates
  - Internal
    - Senior Management
    - Business Units
    - Staff
    - Crisis Management Team
    - Others
  - External
    - Media
    - Law Enforcement
    - Customers
    - Business Partners
    - Vendors
    - Others

g) Michigan Cyber Disruption Response Plan (CDRP) Activation

- Internal conditions and steps necessary to activate the Michigan Cyber Disruption Response Plan.
- Primarily based on organization triage process decision trees.
- Triage process should be fully auditable to ensure appropriate actions and decisions that are made by teams responsible for those actions or decisions.

Annex C: Training and Exercises

C.1 Introduction

This annex provides a training and exercise framework for cyber security professionals charged with the defense of Michigan's critical infrastructure.

C.2 Training Plan

Effective training & exercise plans address the following elements to support the various roles and functions of assigned members:

- Basic and advanced training, including refresher training requirements
    - External training
    - Internal training
    - Certifications gained/maintained
- Process testing training
    - Regular pre-scheduled process training/testing exercises including table-top exercises
    - Random unscheduled process training/testing exercises including table-top exercises

Michigan has defined a set of recommended capabilities associated with seven cyber security domains essential to the protection of critical systems. Critical infrastructure owners and operators must ensure expertise in these seven primary cyber security areas reside within their organization. Development of these capabilities within all partner organizations is the goal. The form those capabilities take, within the organizations, is up to the partners.

The Michigan Cyber Range offers a number of courses that provide training and certifications in the seven core Michigan Cyber Disruption Response Plan training domains. Table C-1 maps domains to course topics and certifications designed to support training plans. More information and a course listing are available at www.merit.edu/cyberrange.

Domains	Course Topics	Cyber Range Certifications
Application Level Security	a. Known Software/Database Vulnerabilities (Java, SQL) b. Web Application Security c. Application Based Attacks (Buffer Overflow, SQL Injection)	Certified Information Systems Security Officer Certified Penetration Testing Consultant Certified Penetration Testing Engineer
Hardware and Device Level Security	a. Vulnerabilities of Routers, Switches, Servers b. Cryptography c. Firewalls	Certified Information Systems Security Officer Certified Penetration Testing Consultant Certified Penetration Testing Engineer
Network Level Security	a. OSI Model and Protocols b. Network Architecture (LAN, Wireless) c. Network Based Attacks (wireless intercept, IP spoofing)	Certified Information Systems Security Officer Certified Penetration Testing Consultant Certified Penetration Testing Engineer
Disaster Recovery and Business Continuity	a. Business Impact Analysis b. Business Continuity Planning c. Interdependency	Certified Disaster Recovery Engineer
Computer Forensics	a. Seizure Concepts b. Incident Investigation c. Digital Evidence and Electronic Discovery	Certified Network Forensics Engineer Certified Digital Forensics Examiner
Physical Security	a. Risks, Threats and Countermeasures b. Physical Intrusion Protection c. Access Control	Certified Information Systems Security Officer
Incident Management	a. Incident Command System b. Roles and Responsibilities c. Incident Reporting	Certified Incident Handling Engineer

Table C-1: Michigan Cyber Disruption Response Training Domains

C.3 Additional Training Resources

In addition to the Michigan Cyber Range, a variety of public and private organizations provide training in the designated training domains in Table C-1, above. Examples of such organizations and training offered include, but are not limited to:

- *Federal Emergency Management Agency (DHS/FEMA) Emergency Management Institute (EMI)* offers a variety of in-residence and online courses in incident management and security and emergency management, including several on continuity and disaster recovery (www.training.DHS/FEMA.gov).

- The *SANS Institute* provides specialized information technology training resources delivered in a variety of formats (www.sans.org).

- The *International Information Systems Security Certification Consortium (ISC2)* offers a number of training and certification (with concentrations) options including the industry leading Certified Information Systems Security Professional (CISSP) designation (www.isc2.org).

- *ISACA* provides guidance, benchmarks, education and certifications for information systems governance, security, audit, and assurance professionals. ISACA security focused certifications include the Certified Information Systems Auditor (CISA) and Certified Information Systems Manager (CISM) designations (www.isaca.org).

C.4 Exercises

DTMB and MSP/EMHSD work in close collaboration to leverage MSP/EMHSD exercise planning and implementation expertise and methodology using the Homeland Security Exercise and Evaluation Program (HSEEP) framework (Figure C-1). HSEEP ensures exercises are conducted according to a standard risk-based methodology applicable to all mission areas: prevention, protection, mitigation, response and recovery.

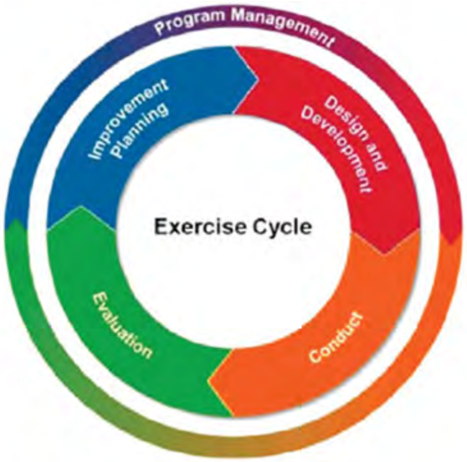


Figure C-1: HSEEP Exercise Cycle

DTMB, MSP/EMHSD and subject matter experts will plan, develop, schedule and execute cyber disruption scenarios for the following types of exercise (as detailed in Appendix C: Exercise Types of the State of Michigan/UASI Training and Exercise Plan). HSEEP exercises are organized in a progressive manner.

- Discussion-Based Exercises
  - Seminars – Generally used to orient participants to or provide an overview of authorities, strategies, plans, policies, procedures, protocols, response resources, or concepts and ideas.
  - Workshops – Similar to seminars with increased interaction and focus on achieving or building a product (such as plan or policy).
  - Tabletop Exercises (TTXs) – Intended to stimulate discussion of various issues regarding a hypothetical situation. Can be used to assess plans, policies,

and procedures or to assess types of systems needed to guide the prevention of, response to, and recovery from a defined incident.

- Operations-Based Exercises

  - Drills – A coordinated, supervised activity usually used to test a single, specific operation or function in a single agency. Commonly used to provide training on new equipment, develop or test new policies or procedures, or practice and maintain current skills.

  - Functional Exercises (FEs) – Also known as a Command Post Exercise (CPX). Focused on exercising the plans, policies, procedures and staffs of the direction and control nodes of the ICS or Unified Command System (UCS).

  - Full-Scale Exercises (FSEs) – Multi-agency, multi-jurisdictional exercises that test many facets of emergency response and recovery. Simulates the reality of operations in multiple functional areas by presenting complex and realistic problems requiring critical thinking, rapid problem solving, and effective responses by trained personnel in a highly stressful environment.

C.5 Exercise Planning Process

MSP (MC3, EMHSD) and DTMB will:

- Determine exercise type/schedule.
- Develop exercise scenarios in collaboration with required subject matter experts.
- Define and coordinate logistics (location, facility, supplies, etc.).
- Coordinate details with the applicable person and/or entity.
- Conduct and evaluate exercise.
- Document findings and recommendations in an after action report and program improvement plan.

Annex D: Risk Assessment

D.1 Risk Management Framework

The adopted risk management framework for the Michigan Cyber Disruption Response Plan is represented in the following graphic:

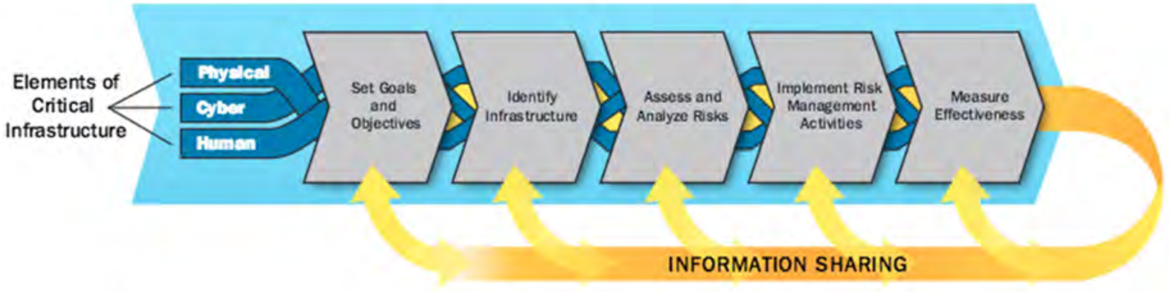


Figure D-1: Risk Management Framework

U.S. Department of Homeland Security, National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, p. 15. (Available at http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf)

The Michigan Cyber Disruption Response Plan sets goals and objectives for the management of cyber disruptions affecting critical systems. The remaining areas of the risk management framework are equally important to the effective management of cyber disruption risk.

D.2 Identification of Critical Network Assets

BIA results for each asset in your asset management system (AMS) should be reviewed to identify and prioritize your organizations most valuable and important (critical) assets. The BIA methodology used should encompass the risk assessment methodology outlined below.

D.3 Risk Assessment Methodology

Risk assessment involves the development of a measure of risk based on the evaluation of the threat, vulnerability and consequences associated with an attack on a target, such as critical infrastructure. Risk assessment is necessary for risk management and typically involves the following steps:

1. Identify critical infrastructure and key resources;
2. Identify and assess threats to the subject infrastructure;
3. Identify the vulnerabilities of the target infrastructure associated with the identified threats;
4. Evaluate the consequences of a successful attack on the subject infrastructure;
5. Determine the risk to the subject infrastructure based on the aforementioned factors;
6. Identify means of reducing risk to subject infrastructure;
7. Evaluate the resources available to mitigate risk; and,
8. Develop a risk management strategy taking into account the risk priorities and resources available.

Common methods for risk assessment include the use of subject matter experts and the scoring of risk characteristics based on relativistic scales. Additionally, penetration testing or "red team" techniques may be used to uncover vulnerabilities and test security of potential targets, yielding data that may be used to develop risk assessments and mitigation priorities.

A common method of risk evaluation is the use of relativistic methodologies. In this approach, various scales are used commonly across all evaluated targets and targets are given a score based on the assessor's determination. Often, individuals conduct these risk assessments with expertise in the given sector in order to support the evaluation's integrity. These scales are typically represented in one of two ways, either by a scoring scale, which applies points to different vulnerabilities, which are later totaled, or by percentage. In the case of percentage the decision factor is often represented as (0,1), meaning the factor should be rated as 0% probably (0) to 100% probable (1). For example, the threat of a vehicle borne improvised explosive device at a particular target site may be assessed by an expert to be 85% likely (.85). The factor can then be applied in a formula upon which the method is based.

R = TxVxC
Where:

- R= Risk (Expected Loss)
- T = Threat
  - (0,1)
  - Likelihood of a potential type of attack
    Intent and capability of the adversary
- V = Vulnerability
  - (0,1)
  - Likelihood or probability of successful attack
- C = Consequence
  - Replacement cost, could be in dollars
  - Direct economic impact
  - Indirect economic impact

The Michigan Cyber Disruption Plan recommends that any risk assessment used by partners is documented, reproducible, and defensible and based on the risk factors indicated above. The results of such risk assessment results can be discussed and shared with partners, as appropriate, to assist in the identification of critical network nodes and their associated interdependencies.

D.4 Prioritized Remediation

Ultimately, the goal of the risk assessment process is to provide a prioritization of the critical assets of Michigan's networks, and a plan to safeguard them. The highest priority assets should be those that are most vulnerable and would have the greatest impact if disrupted. As such, these critical nodes should receive the greatest amount of resource support. Members will develop remediation plans based on their risk assessment activities using a state-wide pre-defined remediation plan format, the key fields include:

Member Name:
Location:
Function:
Risk Identified:
Asset(s) Impacted and their Criticality:
Recommended Remediation Activity:
Date Remediation Activity Approved:
Date Remediation Activity Approved by:
Residual Risk(s) following Remediation Activities:
Date Remedial Recommendation(s) Implemented:
Implementation Team:

These plans will be reported to the CDRP partnership at a level of detail deemed appropriate by the reporting member.

D.5 Measuring Effectiveness

An effective protective program should yield measurable progress. Regular meetings of the Michigan Cyber Disruption Response Plan Partners will include a structured report of the effectiveness of remediation.

Annex E: CDRP Roles and Responsibilities

E.1 Michigan Chief Information Officer (CIO)

When a cybersecurity event escalates to be classified as a cyber-disruption the CIO works with MSP/EMHSD, the SBO, the Chief Technology Officer (CTO) and the Chief Security Officer (CSO) to identify related issues and effects, and assist in the remediation efforts. The CIO is also responsible for communications with high-level political officials and the media.

E.2 Michigan Chief Technology Officer (CTO)

The CTO reports to the CIO and is responsible for state IT infrastructure day-to-day operations. During a cyber-disruption, the CTO works with the CIO, CSO, and MSP/EMHSD to ensure cybersecurity issues and effects are properly identified and remediated. The CTO also collaborates with MSP/EMHSD to establish the SEOC and coordinate mitigation and recovery activities where man-made or natural disasters intersect with a parallel cyber-attack or cyber disruption effort.

E.3 Michigan Chief Security Officer (CSO)

The CSO reports to the CIO and is responsible for protecting the State’s IT infrastructure from internal and external cybersecurity threats. The CSO is also responsible for the state’s cybersecurity readiness, threat analysis, and remediation efforts. This responsibility includes:

- Working with agency IT staff to address local and statewide cybersecurity events.
- Working with MS-ISAC to assist in statewide, regional and national cybersecurity events and to communicate potential remediation procedures to agencies, counties, boroughs, and cities impacted by a cyber-disruption.
- Acting as the MI-ISAC chairman:
  - Ensuring the state or regional ISAC communicates cybersecurity threat levels and provides local readiness and response within the state.
  - Providing a central resource for gathering information on cyber threats to critical infrastructure throughout the state.
  - Facilitating information sharing between local governments and other states encompassed by the event.
- Leading response efforts for cybersecurity events that have statewide implications. During a concurrent cyber-event and emergency event, the CSO and MSP/EMHSD or the Incident Commander will share this role.
- State Emergency Operations Center (SEOC) Cybersecurity Emergency Preparedness Liaison Officer (EPLO) – The CSO is the CIO’s representative at the SEOC during cyber events that reach High or Severe threat level.
- Michigan Emergency Management Plan/Emergency Support Function (MEMP/ESF) #2 (Warning and Communications) – The CSO will ensure the Office for Information Security fulfills the responsibilities identified in the Cyber

Attacks section of the MEMP Technological Disaster Procedures section, maintained by MSP/EMHSD.

- Federal Emergency Management Agency (FEMA) – The CSO, in conjunction with MSP/EMHSD, will work with FEMA to address cybersecurity incidents and disruptions that impact or are precipitated by national disaster recovery efforts.
- U.S. Computer Emergency Readiness Team (US-CERT) – The CSO will ensure the Office for Information Security works with US-CERT to gather and disseminate cybersecurity information and warnings to the state.
- Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD) – The CSO will assist MSP/EMHSD with their mission of enhancing the state’s information and intelligence sharing capabilities with law enforcement on a local, state, and national level, focusing on prevention, protection and mitigation.
- Michigan Intelligence Operations Center (MIOC) and Michigan Cyber Command Center (MC3) – The CSO will work with the MIOC and the MC3 to support their mission of assisting local, state, and federal law enforcement agencies with cyber terrorism and cyber-criminal activity. This assistance may range from providing subject matter experts (SMEs) to assist in the analysis of cyber threat information to providing cybersecurity training for the MIOC and MC3 analysts.
- Service Providers (SP) – The CSO will work with the service providers listed in the state enterprise services portfolio to ensure they perform proper reporting and management of cybersecurity disruptions in order to secure and protect the state’s critical IT business processes and assets from cyber threats.
- Proactive Cybersecurity Event Monitoring – The CSO will use the MS-ISAC, Microsoft Bulletins, and other media outlets to proactively identify potential cybersecurity threats and take precautions before they can cause harm to the state’s IT infrastructure.
- State Security Threat Level – The CSO is responsible for setting and alerting the state regarding the current cybersecurity threat posture.
- Cybersecurity Alerts – The CSO, in partnership with the MC3, disseminates cyber threat warnings and information to state government agencies, local government agencies, private citizens, and business entities.
- Coordinating Recovery From Cybersecurity Attack/Event – During a cyber-event the CSO coordinates the recovery of state network operations, telecommunications, and IT applications and databases.
- Remediation Efforts – The CSO coordinates with local government IT representatives, through the MI-ISAC and ISOs, to exchange policy and operational information required to respond to and recover from cybersecurity incidents.
- Agency Support – The CSO provides assistance to agencies remediating issues caused by cybersecurity incidents.

- Cybersecurity Preparedness and Education – The CSO is responsible for preparing and educating state agencies, and employees to the dangers of cybersecurity threats and how to reduce risk exposure.
- Collaboration – The CSO, in partnership with the MC3, facilitates interaction and collaboration among state agencies, state and local governments, national organizations, business partners, private sector entities, and international organizations related to cybersecurity and cyber incidents.
- Cybersecurity Advanced Analytics – The CSO develops and exercises cybersecurity related predictive analytics capabilities.
- Cybersecurity Forensic Analysis – The CSO supports the Department of Justice, Federal Bureau of Investigations, Michigan State Police and other law enforcement agencies in investigating and gathering information related to cyber threats and attacks.
- Statewide Cybersecurity Emergency Response – The CSO work with MSP/EMHSD to coordinate remediation efforts from a cybersecurity event that jeopardize the health and safety of the citizens of the state. The CSO disseminates cyber threat warning information in conjunction with the SEOC.

E.4 Enterprise Data Center (EDC)

The EDC is responsible for ensuring state servers are patched properly and have the most current antivirus and intrusion detection software installed. During a cybersecurity event, the EDC will work with the CSO to resolve issues that may require initiation of the Disaster Recovery Plan.

E.5 Continuity of Operations Plan Incident Command Team

In the event of activation or partial activation of the Continuity of Operations Plan (COOP), the COOP Incident Command Team has been identified and organized according to federal NIMS/ICS guidelines. To staff the COOP teams, MSP/EMHSD has identified key positions to provide management and technical expertise necessary to establish critical functions within 12 hours after the emergency event.

E.6 Agency Cybersecurity Emergency Preparedness Liaison Officer (Agency Cybersecurity EPLO)

The Agency Cybersecurity EPLO is assigned and authorized, by the respective agency heads, to act as the agency’s cybersecurity representative at the SEOC. During a cybersecurity event, this individual:

- Represents the Agency – The Agency Cybersecurity EPLO represents the agency, from an IT perspective, and has authority to redirect IT personnel, assets, and other resources to the remediation effort.
- Emergency Purchase Orders – The Agency Cybersecurity EPLO completes emergency purchase orders to procure equipment, staff augmentations, backup facilities, services and supplies.

- Enacts the Agency COOP - The Agency Cybersecurity EPLO has the authority to enact the agency's COOP.

E.7 Agency Information Security Officers (ISOs)

ISOs are responsible for the day-to-day IT security administration of their respective agencies. During a cybersecurity event, ISOs report cybersecurity incidents to the CSO. ISOs:

- Monitor their agency's internal cybersecurity level and report increases/decreases to the CSO.
- Report cybersecurity incidents to their agency IT staff and the CSO.
- Communicate security related information to the CSO, agency IT staff, business partners, and users.
- Assist in agency remediation efforts.

E.8 State Government Service Providers

State government service providers support the CSO with the state's cybersecurity mission and perform proper reporting and management of cybersecurity incidents in order to secure and protect the state's critical Information Technology (IT) business processes and assets from cyber-threats. As part of these responsibilities, service providers provide:

- Technical and operational support for the CSO when a cybersecurity incident involves enterprise assets, multiple agencies, or outside entities such as business partners or citizens that are utilizing a service provider's controlled assets (e.g., appliances, servers, firewalls, routers, and other systems), Incident handling processes are outlined in Section 6.4 and 6.5 for service providers and service provider/Level 3 respectively
- Points of contact to be responsible for ensuring that cybersecurity incident reporting and handling is addressed within the timeframes identified by the state's incident response Service Level Agreements (SLAs).
- Notification to DTMB, within thirty (30) minutes of detection, that incident reports need to be filed within four (4) hours of detection.
- Prompt investigation of incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse, or access to information technology resources such as systems, files, and databases.
- Alerts to CSO of potential cybersecurity incidents discovered via their automated incident response, intrusion detection, and security event and incident management systems.
- Names, work phone numbers, mobile phone numbers, home phone numbers, and work and home e-mail addresses for cybersecurity incident responders who can work with CSO to remediate cybersecurity incidents
- Cooperation with CSO cyber incident investigation and remediation efforts.

- Processes for ensuring all service provider security operations and support employees are aware of the state’s cybersecurity policies and procedures.
- Guidance to ensure the service provider security operations and support Service Desk personnel are aware of the internal/external cybersecurity incident response processes and how to differentiate between network, telecom, and cybersecurity incidents.

E.9 State Government Business Partners

State Government Business Partners (BPs) are defined as companies and non-profit organizations that provide support to the state IT infrastructure or require access to provide services to citizens. During a cybersecurity incident, BPs work with the, CIO CTO, and CSO to remediate issues associated with the attack.

E.10 Michigan State Police, Emergency Management and Homeland Security Division (MSP/EMHSD)

The mission of MSP/EMHSD is to coordinate state agency response, including the to support county and local governments in the areas of civil defense, disaster mitigation and preparedness, planning, and response to and recovery from man-made or natural disasters.

MSP/EMHSD manages the overall protection framework and oversees the implementation and continual evaluation of the state’s Critical Infrastructure Protection Program. This program is comprised of five objectives that include: identifying assets; assessing risks; prioritizing disaster recovery; implementing protective programs; and measuring effectiveness.

During a cybersecurity event, MSP/EMHSD monitors the situation to determine if an event is tied to a terrorist attack. If it is, MSP/EMHSD will act as a liaison to the Federal Department of Homeland Security (DHS) to help coordinate federal resources and assist in the recovery process.

From a cybersecurity perspective MSP/EMHSD:

- Works with the county emergency management agencies and communication centers to ensure that MSP/EMHSD’s IT based resources are not impacted by a cyber-security event.
- Coordinates statewide response of the counties and municipalities and collect, report, and remediate any cybersecurity threat that could impact disaster recovery efforts.
- Acts as the state’s backup cybersecurity operations center providing the CIO and agencies, impacted by cybersecurity events, with meeting facilities and back-up communications (satellite feeds, wireless radios, etc.).

E.11 Michigan Information Sharing and Analysis Center (MI-ISAC)

The MI-ISAC is responsible for addressing cybersecurity readiness and critical infrastructure coordination. It is led by the CSO who is responsible for leading the state's efforts for cyber-readiness and resilience. It provides a common mechanism for raising the level of cybersecurity readiness and response within state government by providing a central resource for gathering information on cyber threats to critical infrastructure throughout the state and providing two-way sharing of information between and among local governments.

E.12 Michigan Intelligence Operations Center (MIOC)

The MIOC, operated by the Michigan State police, is the statewide intelligence operations fusion center that provides law enforcement agencies a central point of contact for their information needs. MIOC analysts provide state police members and federal, state, and municipal law enforcement officers with access to intelligence information, investigative data, and public source information 24 hours a day, seven days per week. Analysts also provide investigative support by analyzing complex information and collating it into intelligence summaries, organization charts, link analysis, time event analysis, and other manageable, professional products.

During a cyber event, the MIOC works in conjunction with MC3 and the CSO to help identify, document, and collect forensic evidence for potential prosecution. In addition to this, the MIOC helps coordinate investigations that involve the Department of Homeland Security and the Federal Bureau of Investigation's cyber law enforcement agencies to prosecute cyber criminals that may reside in other states and nation states.

E.13 Michigan Cyber Command Center (MC3)

The MC3 is a specialized group of MSP enlisted and civilian analysts who are highly trained and have legal authority to investigate technology facilitated crimes in partnership with skilled public and private professionals in emergency response to cyber events. The MC3 emphasizes Cyber Crime prevention through information sharing, training, partnerships, and outreach. It functions as the central command and control center during cyber disruption situations having a potential crime nexus. During a Cybersecurity event, the MC3 is responsible for the coordination of Cyber First Responders focusing on minimizing damage, identification of electronic evidence, forensic data recovery and analysis, as well as developing strategies for criminal prosecution while operating under the authority of the SEOC.

E.14 Michigan National Guard Cyber Teams (MI-NGCT)

The Michigan National Guard (NG) is comprised of the Air National Guard (ANG) and Army National Guard (ARNG). In peacetime, the governor serves as commander in chief of the NG, exercising control through the adjutant general. In the event of natural disaster or civil emergency, the governor can order NG personnel and equipment into service to assist state and local authorities. As part of this mission, the NG has created teams of part-time soldiers and airmen who work as cybersecurity experts in the private and public sectors.

During a large scale cyber event, the Governor will activate NG cyber teams to assist state and local governments with combating cyber-attacks and restoring critical physical infrastructure (including dams, power plants, mass transit) and services lost or damaged resulting from cyber-attacks. In addition to recovery, the NG will work with MSP/EMHSD and service providers to establish alternate forms of telecommunications (satellite, cellular, shortwave, etc.) and assist with physical security at critical infrastructure and alternate recovery sites.

E.15 Michigan Cyber Civilian Corps (MiC3)

The Michigan Cyber Civilian Corps (MiC3) provides rapid response to Governor-declared state of emergency cyber events. It consists of volunteer cyber experts, from government, education and business sectors, who work with DTMB, MSP, NG and other public and private sector entities providing mutual aid to government, education and business organizations in the state of Michigan.

E.16 Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a collaborative organization with participation from all 50 states, the District of Columbia, local governments and U.S. Territories. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cybersecurity readiness and response in each state and with local governments.

E.17 DHS/Federal Emergency Management Agency (DHS/FEMA)

DHS/FEMA provides communications and IT support to Joint Field Office operations, and coordinates the restoration of Public Safety Communications systems and first-responder networks. During a cybersecurity event, DHS/FEMA works with the National Communications System (NCS) to provide communications support to the impacted area and assists in the remediation efforts.

E.18 U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT is a 24/7 operations center with connectivity to all major federal cyber operations centers, private sector Internet service providers, information sharing mechanisms, and vendors. During a cyber-event, US-CERT acts as a focal point to collect and disseminate cybersecurity information received from public and private sector sources.

Annex F: Glossary

Abbreviation	**Definition**
A	
ANG	Air National Guard
AMS	Asset Management System
APT	Advanced Persistent Threat
ARNG	Army National Guard
ASEOC	Alternate State Emergency Operations Center
B	
BCP	Business Continuity Plan
BIA	Business Impact Assessment
BP	Business Partner
C	
CDRP	Cyber Disruption Response Plan
CDRT	Cyber Disruption Response Team
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISM	Certified Information Systems Manager
CISSP	Certified Information Systems Security Professional
COG	Continuance of Government
ConOps	Concept of Operations
COOP	Continuity of Operations Plan
CPX	Command Post Exercise
CSO	Chief Security Officer
CTO	Chief Technology Officer
D	
DHS	Department of Homeland Security
DR	Disaster Recovery
DTMB	Department of Technology, Management and Budget
E	
EDC	Enterprise Data Center
EM	Emergency Management
EMI	Emergency Management Institute
EPLO	Emergency Preparedness Liaison Officer
ESF-2	Emergency Support Functions – Communications

F

FBI	Federal Bureau of Investigation
FE	Functional Exercise
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FSE	Full-Scale Exercise

G

H

HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network

I

IAP	Incident Action Plan
ICS	Incident Command System
IIS	Internet Information Services
IOC	Indicators of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
(ISC)2	International Information Systems Security Certification Consortium
ISO	Information Security Officer
IT	Information Technology

J

K

L

M

MC3	Michigan Cyber Command Center
MEMP/ESF	Michigan Emergency Management Plan/Emergency Support Function
MiC3	Michigan Cyber Civilian Corps
MI-ICS	Michigan-wide Incident Command System
MI-ISAC	Michigan Information Sharing and Analysis Center
MING	Michigan National Guard
MI-NGCT	Michigan National Guard Cyber Teams
MIOC	Michigan Intelligence Operations Center
MOM	Microsoft Operations Manager

MS-ISAC	Multi-State Information Sharing and Analysis Center
MSP	Michigan State Police
MSP/EMHSD	Michigan State Police, Emergency Management and Homeland Security Division

N

NCS	National Communications System
NG	National Guard
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NSA	National Security Agency

O

OP	Operational Period

P

Q

R

RTO	Recovery Time Objective

S

SBO	State Budget Office
SCADA	Supervisory Control and Data Acquisition
SEOC	State Emergency Operations Center
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Center
SOS	Security Operations and Support
SP	Service Provider

T

TTX	Tabletop Exercise

U

UASI	Urban Areas Security Initiative
UPS	Uninterrupted Power Supply
US-CERT	United State Computer Emergency Response Team

V

VOIP	Voice Over Internet Protocol

W, X, Y, Z

SPECIAL THANKS TO THE CIO AND CSO KITCHEN CABINETS FOR THEIR PARTNERSHIP

Amerisure
Beaumont Health Systems
Blue Cross Blue Shield
Board of Water & Light
BorgWarner
CGS Advisors
Chrysler
City of Detroit
City of Detroit Water & Sewage
CMS Energy
Dow
DTE Energy
Education Achievement Authority of Michigan
Federal Mogul
Flagstar Bank
Homedics
Kent County
Meridian Health Plan
MGM Grand Detroit
Michigan Health Cybersecurity Council
Michigan State University
Nexteer Automotive
Oakland County
Penske
Plante Moran
Quicken Loans
Sparrow
University of Michigan
ZF Group

THE STATE OF MICHIGAN

E PLURIBUS UNUM

TUEBOR

SI QUÆRIS PENINSULAM AMŒNAM

CIRCUMSPICE

A.D. MDCCCXXXV.